State of Iowa
Department of Administrative Services
Information Technology Enterprise (ITE)

Security Policy Manual

June 2011

ITE Security Policy Manual

Foreword

The Department of Administrative Services (DAS) Information Technology Enterprise (ITE) Security Policy Manual is intended for DAS-ITE employees and contractors. Information throughout the manual supports the DAS mission by providing direction and guidance to protect DAS resources. It establishes uniform policies and responsibilities for carrying out the DAS-ITE Security Program. Security is provided for information that is collected, processed, transmitted, stored, or distributed for all other governmental entities utilizing ITE general support systems and major applications.

Additional copies may be obtained from the Information Security Office, Department of Administrative Services, Hoover State Office Building, Level B, Des Moines, IA 50319 or by e-mailing jeff.franklin@iowa.gov.

Signed,

Lorrie Tritch
Chief Operating Officer (COO)
Department of Administrative Services
Information Technology Enterprise
Hoover State Office Building - Level B
Des Moines, IA 50319
e-mail: Lorrie.Tritch@iowa.gov

Table of Contents

Section	Page
Chapter 1 - Introduction	4
Chapter 2 - Enterprise Policies and Standards	6
2.1 Enterprise Information Security Policy	6
2.2 Enterprise Wireless LAN Standard	9
2.3 Enterprise Removable Storage Encryption Standard	12
2.4 Enterprise Laptop Data Protection Standard	13
2.5 Enterprise Data Classification Standard	15
2.6 Enterprise Interconnectivity Standard	16
2.7 Shared Authentication Standard	20
2.8 Enterprise Mobile Device	23
2.9 Data Stewardship	25
2.10 Compliance	27
2.10 Web Application	28
Chapter 3 - DAS-ITE Operating Security Policy	31
Chapter 4 - DAS Work Rules	41
4.1 Computer Security	41
4.2 Confidentiality	41
4.3 Internet and Email	42
4.4 Visitor Security Assurance Policy	43
Chapter 5 - State of Iowa Employee Handbook	45
Chapter 6 - Iowa Law	46
Chapter 7 - Physical Security	51
Chapter 8 - Computer Security Incident Response	54
Chapter 9 - DAS PCI Policy Statement	58
Chapter 10 - Mainframe Security	64
Glossary	65
Appendix A - Roles and Responsibilities	67
Appendix B - Sample Breach Notification	70
Appendix C - Acknowledgment of Receipt for the ITE Security Policy Manual	71

CHAPTER 1 - INTRODUCTION

1.1 PURPOSE

This manual combines security rules and procedures from a variety of sources including: enterprise standards; departmental operating policies; departmental work rules; departmental standard operating procedures; and state law into a consolidated security policy. The Security Policy Manual promotes the Department of Administrative Services - Information Technology Enterprise (DAS-ITE) mission and provides guidance for protecting the confidentiality, integrity and availability of governmental information systems.

DAS-ITE information systems security policies are consistent with state and federal: law, policies, standards, and procedures.

1.2 DEFINITIONS

Appear in the Glossary at the end of this manual.

1.3 SCOPE

This policy manual consolidates the information security policies applicable to the Department of Administrative Services Information Technology Enterprise (DAS-ITE). This document applies all DAS-ITE personnel, including contractors acting for DAS-ITE, and all authorized users who access DAS-ITE information systems, networks, and support facilities. Policy provisions also apply to non-DAS-ITE organizations, or their representatives, who are granted access to DAS-ITE information systems resources, including other government agencies.

This policy manual excludes microprocessors embedded in or dedicated to production or process control equipment (e.g., building automation and building maintenance equipment).

1.4 BACKGROUND

DAS Mission:

“The mission of the Department of Administrative Services, as it relates to information technology services, is to provide high-quality, customer-focused information technology services and business solutions to government and to citizens.” [Iowa Code 8A.202(1)]

Government employees and contractors use DAS-ITE information systems for all facets of state government operations. DAS-ITE information systems support law enforcement efforts, agency activities, and provide services and information to the residents of Iowa.

Information Security Office:

The Information Security Office is responsible for developing, implementing and distributing information security policies, standards, and practices that protect the confidentiality, integrity and availability of computer systems, and for promoting enterprise-wide compliance with security requirements.

The Information Security Office provides security awareness training materials as part of its education and outreach program. The ISO is responsible for computer security incident response coordination and monitors and analyzes security alerts and security best practices information and distributes them to DAS-ITE staff as appropriate.

Security Classification:

(a) Unless otherwise designated, DAS-ITE general support systems and major applications are considered to contain confidential information.

(b) All applications, and automated information systems containing Federal data must be afforded adequate security. [OMB A-130,AIII]

(c) Those agencies or agents that receive FTI directly from either the IRS or from secondary sources (e.g., Health and Human Services, Federal entitlement and lending agencies) must have adequate programs in place to protect the data received. [IRS Publication 1075]

Policy Application and Organizational Structure

DAS-ITE information system security includes applicable security life-cycle requirements. Additional related programs are incorporated in this document by reference and should be considered when establishing and reviewing DAS-ITE information system security requirements. Their applicable policies and procedures may be obtained via the appropriate DAS-ITE Division Administrators/Managers.

1.5 ROLES AND RESPONSIBILITIES

Information assurance requires the active support and ongoing participation of all involved parties. It requires support from the executive level and universal compliance. Responsibility for satisfying policy requirements is shared and extends to all personnel involved with the development, implementation, operations, use, and maintenance of government information systems. Each person shall satisfy the requirements as they relate to the portion of each information system under their control. Implementation, acceptance, and maintenance of adequate system and network security is a shared responsibility of senior management, project managers, security and system administrators, supporting and using organizations, technology providers, and users. Senior managers, project managers, technical staff, and security personnel are responsible for evaluating the level of risk associated with any particular information system and implementing adequate security controls to reduce the risk to an acceptable level. Specific roles and responsibilities, both at the management and staff level, are listed in Appendix A.

1.6 UPDATES

The Security Policy Manual will be reviewed annually and updated as needed.

1.7 Violations

Violations of these policies may subject staff to employee disciplinary action.

CHAPTER 2 - ENTERPRISE POLICIES & STANDARDS

Enterprise security standards apply to all state agencies including DAS-ITE. The goal of the enterprise policies and standards is to provide a minimum level of security that is consistently applied across agencies. Enterprise standards are developed in a collaborative manner with participants from various state agencies.

Current State of Iowa enterprise security policies and standards include:

- State of Iowa Enterprise Information Security Policy;
- State of Iowa Enterprise Wireless LAN Standard;
- State of Iowa Enterprise Removable Storage Encryption Standard;
- State of Iowa Enterprise Laptop Data Protection Standard;
- State of Iowa Enterprise Data Classification Standard;
- State of Iowa Interconnectivity Standard;
- State of Iowa Shared Authentication Standard;
- State of Iowa Enterprise Mobile Device Standard;
- State of Iowa Enterprise Data Stewardship Standard; and
- State of Iowa Enterprise Application Security Standard.

The complete enterprise security standards are located at:

http://das.ite.iowa.gov/standards/enterprise_it/index.html

The key provisions of each standard are listed below.

2.1 Enterprise Information Security Policy

The Enterprise Information Security Policy establishes the overarching information security policy for the State of Iowa. It is broad in scope and is supplemented by additional enterprise security policies. It is the Information Security Standard of the State of Iowa that:

1. Trusted Environment: Each agency operates in a manner consistent with the maintenance of a shared, trusted environment within state government. Agencies shall not jeopardize the confidentiality, integrity or availability of state computing systems; or the information stored, processed and transmitted by any state information system.

2. Enterprise Standards: Each agency follows established enterprise security standards except where agency policy provides a higher level of security.

3. Policy: Each agency is responsible for developing policies, processes and procedures to meet this standard. Agency policies may be more stringent than the Enterprise standard. All employees, including interns, contractors, temporary and part-time employees, must agree (in writing or electronically) to follow state and agency security policies before being authorized to access state computer resources.

4. Continuity Plan: Each agency will develop, implement, and exercise an agency business continuity plan. The plan will be based on asset criticality and be consistent with the enterprise continuity of operations plan.

5. Training: Each agency will implement a security awareness/training program for all staff. New employees will be provided basic information technology security training within three months of employment. Additional training, commensurate with the employee's work duties, will be provided annually.

6. Audits: Each agency is subject to a periodic security audit to ensure compliance with this and other enterprise level policies, standards, processes and procedures. An audit or review performed under another authority, such as the Internal Revenue Service, may be substituted if similar in scope and approved by the Chief Information Security Officer.

7. Vulnerability Assessment: Each agency will have a vulnerability assessment performed on its information systems at least annually to gauge the effectiveness of security measures. Assessment results shall be used to help identify, prioritize, plan for and implement additional security measures.

8. Risk Assessment: Each agency will have an information systems risk assessment performed at least every two years. This assessment will be used to help identify, prioritize, plan for and implement additional security measures. The assessment methodology will be developed by the Information Security Office and made available to the enterprise.

9. System Development Life Cycle: Security requirements will be formally defined and addressed throughout the life cycle of all information technology projects, including business requirements definition, design, development, testing, implementation and operation.

10. Agency Compliance: Each agency Chief Information Officer will assure to the best of his or her ability that information systems under their control meet enterprise and agency security policies, standards, processes and procedures prior to being placed in production or after significant changes to the system. The Information Security Office may randomly assess the self-certification process and individual systems to ensure adherence to policy.

11. Privacy: Confidential information that could affect individual privacy will be protected at all times.

12. Monitoring: Monitoring of information system usage for malicious activity and misuse of government resources will be conducted by agencies, or by the Department of Administrative Services, the Iowa Communications Network or other party at the request of the agency.

13. Incidents: Agencies shall report information security incidents that impact, or have the potential to impact, state shared resources to the Information Security Office following a common response plan.

14. Physical Protection: Agencies shall ensure that computer resources and physical information, including but not limited to servers, desktops, laptops, network equipment, firewalls, hardcopies and tapes, have appropriate physical protections in place. Where possible, these resources should also be protected from structural and environmental threats.

15. Network Connections: Agencies will provide information to the Information Security Office describing all connections from their agency networks to outside resources including the Department of Administrative Services shared campus network, the Iowa Communications Network, private service providers, federal, local and municipal governments and other state agencies. Updates will be provided as changes occur.

16. System Updates: Agencies will develop procedures for implementing timely system patches, configuration updates, and other measures necessary to protect systems. The procedures will provide for adequate testing prior to implementation.

17. Security Program: Agencies shall designate a person(s) responsible for coordinating the information technology security functions within the agency and for implementing the agency's information technology security policies.

18. Metrics: Agencies shall develop metrics to be used in measuring the effectiveness of their information security program, standards and practices. The DAS Information Security Office will provide assistance to agencies in developing metrics.

19. Variances: Requests for a variance from any of the requirements of this policy will be submitted in writing by the agency director to the Chief Information Security Officer prior to implementation.

2.2 Enterprise Wireless LAN Standard

The enterprise wireless LAN standard provides state agencies with the minimum requirements for installing and operating a wireless local area network (WLAN). The following minimum standards must be met for all WLANs:

1. **Policy**. Agencies shall establish a WLAN security policy.

2. **Registration.** Agencies shall notify the DAS Chief Information Security Officer prior to implementation of a wireless access point. The notification must include the following for each access point:
   a. Brand,
   b. Model,
   c. SSID and BSSID, and
   d. Physical location.

   The notification must also include the agency name and contact. Non-registered access points are not permitted and shall be removed from service.

3. **Separation of Wireless and Wired Networks.** Wireless network zones must be separated from wired network zones by a firewall or other packet filtering device.

4. **Critical Devices.** Servers and related devices critical to the operation of the agency are not allowed to be hosted from wireless network zones.

5. **Physical Protection.** Wireless access points must be physically protected to limit risk of theft, damage, unauthorized access or configuration reset.

6. **Passwords.** Strong passwords (i.e., alphanumeric with a special characters) shall be used. Two-factor authentication should be considered in addition to strong passwords.
   a. Default administrative passwords used to manage the AP shall be changed.
   b. Administrative passwords shall be at least 15 characters in length.
   c. User passwords to access the wireless shall be at least 8 characters in length.

7. **Access Point Configuration.** Access points shall, at a minimum, meet the following requirements:

   - **Encryption.** Access points purchased after the effective date of this standard must use WPA2-Enterprise or higher encryption. Encryption settings shall be set for the strongest encryption available in the product. Wired Equivalent Privacy (WEP) shall NOT be used.

   - **Service Set Identifier.** The SSID shall be changed from the factory default setting

   - **Beacon Intervals.** Beacon frames shall be set to the maximum interval length.

   - **Cryptographic Keys.** Default cryptographic keys shall be changed before implementation.

- **Address Filtering.** Media Access Control (MAC) address filtering shall be enabled whenever possible. Only connections from recognized MAC addresses should be accepted by the AP.

- **Simple Network Management Protocol Version 3.** If SNMP is needed Version 3 or later shall be used. The default SNMP community string must be changed to a strong community string. Privileges should be set to "read only" if that is the only access required. Unneeded access ports and protocols should be disabled.

- **Channels.** Channels should be set to minimize interference.

- **Range**. The radio frequency power level should be reduced to the minimum level needed and directional antennas used, where practical, to limit the access point range.

8. **Operating Logs.** Wireless access points, where possible, must be set to log operating events including: login attempts (both successful and failed), errors, and reboots. The logs should be maintained on a separate file server. Logs must be reviewed on a regular basis.

9. **Infrastructure Configuration:** The wireless access point shall be configured for infrastructure mode. Ad-Hoc mode allowing peer-to-peer communications between devices is not allowed.

10. **Intrusion Detection.** An intrusion detection/prevention system shall be used to detect unauthorized access attempts or inappropriate use.

11. **Updates**. All components shall have the latest security patches, upgrades and firmware updates.

12. **Assessment.** The DAS Information Security Office may assess state facilities to determine if unauthorized or improperly configured wireless local area networks are present and provide access to agency systems or information. Unauthorized WLANs shall be removed by the agency.

13. **Equipment Disposal**. All sensitive data and configuration information must be removed from wireless components before disposal. For example devices could be reset to factory default settings.

14. **Client Security Maintained.** All computers connecting to the wireless network intended for use by agency personnel must have a properly-configured, host-based firewall, up-to-date antivirus software and be compliant with applicable enterprise and agency standards. Software patches must be applied per the agency's patching schedule.

15. **Awareness Training:** Wireless users shall be provided with wireless security awareness training, including but not limited to documentation describing wireless computing risks.

16. **Public Wireless Network**. Public wireless networks established by agencies shall:
    a. Be isolated outside the logical & physical boundary of the agency network. For example be a separate feed provided by the ICN or a commercial ISP.

b. Agencies may choose to require a user ID and password for access,

Items 6c, 7, 8, 10, 14, & 15 of this standard DO NOT apply to public wireless networks but following them, where feasible, is encouraged.

2.3 Enterprise Removable Storage Encryption Standard

The enterprise removable storage encryption standard establishes the encryption requirements for removable devices and media such as USB flash drives. The minimum standards for removable storage devices and media are:

1. **Policy:** Agencies shall establish a policy covering the use of removable storage devices and media. At a minimum the policy shall cover:
    a. The types of data permitted on removable storage devices and media.
    b. The types of devices permitted.
    c. Reporting of lost or stolen devices.

2. **Data Encryption:** Confidential data stored on removable storage devices and media must be encrypted.

    - The encryption shall be with the Advanced Encryption Standard (AES[1]) cipher using at least a 256-bit key length.
    - A strong pass phrase for accessing encrypted data must be used; at least 8 characters, a mix of numbers and letters with at least one special character.
    - The encryption process shall be centrally managed at the agency and/or enterprise level.

3. **Physical Protection:** Users of removable storage devices and media are responsible for their physical protection.

4. **Primary Storage/Data Backups:** To ensure data availability in the event of device loss or theft, removable storage devices and media should not be the primary storage device for any State of Iowa data. If removable storage devices and media are primary storage for critical data, frequent and regular backups of the data should occur according to agency policy.

5. **Assessment:** The ISO will periodically assess agency compliance with this standard. Agencies will provide access to inventory information and systems as required to determine compliance. If violations of this standard are identified, the agency will receive written notification pursuant to IAC 11--25.11(8A).

6. **Awareness Training:** Staff shall be provided with removable storage device and media security awareness training. At a minimum, users shall be provided with documentation describing removable storage devices and media risks.

[1] Prior to its adoption by NIST in 2000 with the issuance of FIPS 197, AES was commonly known as the Rijndael block cipher.

2.4 Enterprise Laptop Data Protection Standard

The enterprise laptop data protection standard creates the encryption and data protection standard for laptop computers working with state data or connecting to state systems. The minimum standards for all laptop computers are:

1. **Laptop Inventory.** Agencies will maintain an inventory of all laptop computers and their assigned user.

2. **Data Encryption and Authentication.** All laptop computers must be encrypted. The encryption software must meet the following criteria:
    a. Pre-boot: Pre-boot user authentication must be used by the encryption software.
    b. Whole-disk: The entire hard drive shall be encrypted.
    c. Encryption Strength: 256-bit Advanced Encryption Standard (AES) or stronger encryption must be used.
    d. Audit Trail: An audit trail shall be maintained to demonstrate that a device was encrypted and the type of encryption software used.
    e. Central Management: The encryption process and procedures shall be centrally managed at the agency and/or enterprise level.
    f. Hibernation: Laptop encrypts upon hibernation requiring the user to re-authenticate.

3. **Loss/Theft Procedures.** Loss or theft of any laptop computer shall be reported to the Chief Information Security Officer within 24 hours. The notification shall include:
    a. Agency name and contact.
    b. Date of theft/loss.
    c. Description of the theft/loss.
    d. Whether confidential/sensitive information was stored on the device.
    e. Whether the laptop was encrypted.

Procedures should also be in place to change authentication credentials to any systems the device may have accessed; including non-state-owned as well as state-owned devices which store sensitive or confidential data.

4. **Physical Protection.** Users of laptop computers are responsible for their physical protection.
    a. Use of cable locks and other physical security devices are encouraged where appropriate.
    b. Laptops shall not be left unattended in unlocked vehicles.

5. **Passwords**: Strong passwords must be used with laptops. Written passwords, smart cards, or tokens shall not be stored with the laptop.

6. **Primary Storage/Data Backups.** To ensure data availability in the event of device loss or theft, a laptop computer should not be the only or primary storage device for State of Iowa data. Frequent and regular backups of data stored on laptops must be made, according to agency policy.

7. **Client security maintained.** All laptop computers must have:
    a. A properly-configured host-based firewall;
    b. Up-to-date antivirus software; and

c. The latest software patches.

8. **Assessment.** The ISO will periodically conduct assessments of agency compliance with this standard. Agencies will provide access to inventory information and systems as required to determine compliance. If violations of the laptop computer standard are identified, the agency will receive written notification pursuant to IAC 11--25.11(8A).

9. **Awareness Training:** Laptop computer users shall be provided with mobile security awareness training. At a minimum, users shall be provided with documentation describing mobile computing risks.

2.5 Enterprise Data Classification Standard

The enterprise data classification standard requires agencies to review the data they collect and classify it according to the level of protection needed. The classification standard requirements are:

1. **Data Classification.** All data must be classified by the level of protection required. At a minimum data must be classified as either:
   a. Confidential – Information protected by state or federal law, or
   b. Public – Information not included in a protected classification.

   Additional classifications may be used to meet agency requirements. For example, some organizations may use the category of:
   a. Sensitive: Not explicitly protected by law, but exposure could result in negative impact to government services, state government partners or citizens.

2. Data Protection: Agencies shall set protection requirements for each data classification level. Protections should consider different states of data (i.e. at rest, in transit and in use) and forms of data (electronic and paper).

3. Reviews. Agencies shall review their data classification system, and the information they collect, annually to ensure that the data classification levels remain valid.

4. Assessment. The ISO may assess agency compliance with this standard. Agencies will provide access to their classification standard and documentation on how specific data are classified. If violations of this standard are identified, the agency will receive written notification pursuant to IAC 11--25.11(8A).

5. **Notification:** On or before the effective date of this standard, agencies will provide the Chief Information Security Officer with a description of how they are classifying data and a description of the agency standard for protecting data in each classification type.

2.6 Enterprise Interconnectivity Standard

The enterprise interconnectivity standard sets out the requirements for state agencies connecting to the State's shared IT infrastructure. The following are the minimum standards which must be met by agencies connecting to the shared State IT infrastructure.

1. Auditing: All agencies shall maintain and analyze audit logs to detect and track unusual or suspicious activities.

- Develop a log review policy. Include:
  - Length of time for log retention consistent with agency activities and regulations.
  - Individual(s) responsible for log review.
  - Log review procedures including frequency of review.
- Develop baseline behavior for normal activity.

2. Communication: All agencies shall maintain communication with the Information Security Office and exchange information regularly with the Chief Information Security Officer who will in turn relay information to other agencies.

Information to be shared includes:

- Changes in management and technical personnel.
- Activities establishing, maintaining, or terminating interconnections.
- Security incidents affecting the connected systems and data.
- Disasters and other contingencies disrupting any of the connected systems.
- Planned restoration of any interconnection.

3. Emergency Disconnection: All agencies are subject to emergency disconnection from the shared State IT infrastructure.

Agencies may be disconnected after consultation with appropriate staff if:

- Their system is exploited by a virus/worm and no patch is available.
- Their system is an originator of a virus/worm and there is a high risk of infecting other systems.
- The agency is unable to resolve the issue.

Prior to disconnection agencies shall be:

- Given the opportunity to isolate and investigate the incident.
- Notified by telephone or other verbal method, and receive e-mail confirmation of the notification.
- Provided details on when and under what conditions the interconnection shall be restored.
- Except if an agency cannot be reached and an emergency exists.

4. Encryption: Agencies connecting remotely must use encryption for connection, as well as for all remote administration tasks and file transfers.

Encryption is required for:

- Virtual Private Network (VPN) connections.
- Remote administration and file transfers.

5. Firewalls: All agencies shall install firewalls at all interconnections between their agency and other agencies, third party organizations and the Internet.

- Default passwords for all firewalls must be changed before installation.
- Firewall software and/or integrated operating systems of hardware firewalls must be up to date.
- Firewalls must be configured to deny by default all incoming and outgoing transmissions.
- Only required ports shall be opened.
- Critical systems should be segregated from other systems where possible. For example use of a DMZ for web servers.
- Firewall software updates must be tested before going into production.
- Default SNMP community strings should be changed from default for all SNMP manageable devices.

6. Identification and Authentication: Agencies shall identify and authenticate users to ensure that they are authorized to access the interconnection at a minimum implementing a strong password and user ID mechanism.

Mechanisms include:

- User identification and passwords.
    - Passwords are at least eight characters.
    - Passwords are a mixture of alphabetic and numeric characters.
    - Passwords are changed at intervals of sixty days or less.
    - Master password files are encrypted and protected from unauthorized access.
- Digital certificates.
- Authentication tokens.
- Biometrics.
- Smart cards.

The mechanisms may be used by themselves or as part of multi-factor authentication.

7. Logical Access Controls: Agencies shall use Access Control Lists (ACL) and access rules to specify the access privileges of authorized personnel (or agencies if they are using a site-to-site VPN) including the level of access and the types of transactions and functions that are permitted (e.g., read, write, execute, delete, create, and search).

- ACL's should be:
    - Configured offline.
    - Versioned in a repository.

    - Distributed to the appropriate control device.
- Agencies shall grant appropriate access privileges:
    - Based on roles or job functions.
    - Based on the principle of least privilege.
- Only system administrators have access to the controls.
- A log-on warning banner approved by the agency's legal counsel shall notify users that:
    - They have accessed a State of Iowa computer system.
    - Consent to monitoring.

8. Operational Testing: Agencies shall test the interface between applications across all interconnections.

To the extent possible, agencies will test interfaces prior to establishing interconnections.

- Test security controls under realistic conditions.
- Testing shall be conducted in an isolated, non-operational environment if possible.
- Tests and the results should be documented.

9. Patch Management: All agencies must patch their systems in a timely manner.

All agencies shall establish a patch methodology.

- Patches shall be tested prior to being applied.
- Patches deemed critical by the Information Security Office (ISO) applied within five (5) work days of release by the vendor.
- ISO will notify agencies of critical patches via the Security Alert listserv or other means if email is unavailable.
- Non-critical patches shall be applied per a schedule established by the agency.

10. Physical Security: Agencies shall provide appropriate physical security for their information technology systems to prevent unauthorized access.

11. Reporting and Responding to Security Incidents: All agencies shall notify the Information Security Office of intrusions, attacks, or internal security breaches, so that other agencies can take steps to determine whether their systems have been compromised.

- The Information Security Office shall establish a reporting mechanism for agencies.
- The Information Security Office will notify agencies of incidents.
- Agencies shall take appropriate steps to isolate and respond to incidents originating from their systems.
- When appropriate, law enforcement authorities shall be notified, and all attempts should be made to preserve evidence.

12. Security Awareness and Training: Agencies shall conduct security awareness activities and training for all personnel involved in managing, using, and/or operating the interconnection.

- Provide training for new users and refresher training for all users on an annual basis.
- Establish an acceptable use policy and distribute it to all users.
- Require all users to acknowledge acceptable use rules.

13. Security Reviews: Each agency shall review their security controls at least annually, or whenever a significant change occurs, to ensure they are operating properly and are providing appropriate levels of protection.

- Annual vulnerability assessment.
- Security problems shall be documented and corrected in a timely manner.

14. Virus Scanning: Agencies shall install anti-virus software to protect all servers and computer workstations linked to the interconnection.

- Data passing between systems is scanned.
- Anti-virus software automatically checks for updates at least daily.
- Administrators are automatically notified if a detected virus cannot be cleaned.
- Users are instructed on how to report a suspected virus.
- Develop procedures and assign responsibilities for response and recovery.

2.7 Shared Authentication Standard

The shared authentication standard establishes shared authentication requirements for State of Iowa agencies. Shared authentication is a pre-requisite for integration of State computing resources and sharing of data.

Authentication Standard

Centralized Account Repository

State systems that are covered by this Standard ("Systems", herein) will store user credentials in a centralized repository. State and non-State accounts will be made available to any application that uses the repository. Each account should be assigned to a single person, not a group or entity, to maintain the integrity of each account and the secrecy of its password.

The repository will provide the following basic operations:

- Encryption and comparison of the shared secret (password)
- Aging of the password and enforcement of password changing rules
- Flexible password complexity rules
- Open standards for accessing account information (e.g., ODBC, LDAP, etc.)

The repository will integrate with existing State accounts (AD Domains) wherever possible to provide use of those accounts as credentials.

Multi-Factor Authentication

Use of multi-factor authentication provides a higher level of protection for Systems. Using multiple factors can also increase the cost and difficulty associated with using a System. Agencies should balance the risk of unauthorized access to their data against the cost of implementing an authentication method(s). In addition, certain types of data carry specific requirements based on industry, Federal or State standards. Examples of multi-factor authentication bundles include:

- User ID & Password + Secret Questions
- User ID & Password + Certificate
- User ID & Password + Token Generator
- User ID & Password + Token Generator + Certificate

Standard Credential Types

This section outlines the standard credential types for Shared Authentication. After a brief description of the credential type, the pros and cons of that type are listed. Each credential type includes a color-coded table that identifies *relative* values for the following:

- **Cost**: The cost to the State for implementing a centralized credential of this type. Also refers to the per-unit provisioning cost.
- **Strength**: The difficulty with which the credential can be obtained illicitly, stolen, or forged.

- **Factor**: What kind of credential: Something the user *knows*, *has*, or *is*.

1. User ID and Password

Cost: LOW	**Strength: LOW**	**Factor: KNOW**

A user-selected identifier with the suffix @IowaID for external users and *.iowa.gov or *.state.ia.us for State users, and a password that follows the existing State (or Agency) Information Security policy for complexity, aging and history.

The default value for a given user ID will be firstname.lastname@IowaID, but it must be unique and may be edited at registration-time. User IDs will not be re-usable: that is, if an account is deactivated for some reason, no one else will be able to use that same ID, ever. Inactive User IDs will be kept in the centralized repository for this purpose.

By default, passwords for self-registered Accounts will not expire. User's participating in an in-person verification process will be marked as "in-person verified". The expiration flag will be set for "in-person verified users", and the Account's password will be governed according to the State standard for password aging. Password complexity and history requirements will be the same in either case.

Pros:

- Portable
- Nothing to install
- Familiar to users

Cons:

- Difficult to detect theft
- Difficult for users to maintain secure passwords

2. Secret Questions

Cost: LOW	**Strength: LOW**	**Factor: KNOW**

User-selected questions and answers. The answers are stored like passwords, encrypted in the repository. Two questions are selected from a list of common examples, and the third question is entered by the user. The user must enter each answer twice, since the fields are masked and cannot be read (like password fields).

Pros:

- Portable
- Nothing to install
- Somewhat familiar to users

Cons:

- Difficult to detect theft
- Users can forget their answers

3. Certificate

Cost: MED	**Strength: LOW**	**Factor: HAVE**

A State-issued data file that contains encrypted data. Certificates can be installed to a web browser and submitted automatically with web page requests to validate the requestor. A certificate can be proven to have been issued by the State or not.

Pros:

- Semi-portable: Can be installed to multiple computers (work, home, etc.)
- Automatically used when installed

Cons:

- Requires installation by the user
- Difficult to detect theft
- Does NOT prove who the user is, just that they HAVE the certificate

4. Token Generator

Cost: MED	**Strength: MED**	**Factor: HAVE**

A random-number generator that creates a new password every few seconds.

Pros:

- Portable
- Nothing to install
- Prevents “replay” attacks
- Provides non-repudiation

Cons:

- Requires a physical token
- Tokens are expensive ($50-$100)

2.8 Enterprise Mobile Device Security Standard

The Mobile Device Security Standard establishes a consistent set of security practices for the use of mobile devices, such as the Blackberry and other smartphones, by state agencies and contractors. The following elements apply to all agency staff/contractors conducting state business on a mobile device.

1. Passwords/PINs: Passwords/PINs must be enabled for each device. Passwords/PINs must have a minimum length of 4 characters.

2. Erase Data and Disable Device: The device must have the ability to be remotely erased and disabled:

a. After 10 unsuccessful password attempts.

b. When reported lost or stolen.

3. Inactivity: The device must be set to lock after a maximum of 15 minutes of inactivity.

4. Emanations Security: The wireless functionality of devices must be disabled when in areas displaying, storing or transmitting confidential information.

5. Usage Policy: Agencies must:

a. Have a policy covering the use of devices, and

b. Ensure that staff receive and acknowledge the policy.

6. Training: Users are required to receive security awareness training covering use of mobile devices.

7. Short Message Service (SMS): Confidential information shall not be sent by SMS.

8. Peer to Peer Messaging (PIN to PIN): Confidential information shall not be sent by peer-to-peer messaging.

9. Security Patches: Software upgrades and security patches must be applied in a timely manner.

10. **Personally Owned Devices**: Personally owned devices connected to the enterprise email system:

a. Must have the latest security patches installed in a timely manner.

b. Are subject to all of the elements of this standard.

c. Must be erased when the person leaves state government or the device is no longer used for state business.

11. Third Party Applications: Users may not download third-party applications to their device without prior approval.

12. Camera: Use of the camera feature is prohibited in areas displaying, storing or transmitting confidential information including health information.

13. **Reporting**: Users must report lost, stolen or missing devices to their agency, the Service Desk, and the Information Security Office. Notification shall take place as soon as possible, but no later than 24 hours, after the device is discovered to be missing.

14. Bluetooth: The following settings are required for devices using Bluetooth:

a. Disable Discovery Mode,

b. Pairing,

i. Attempts to pair devices require prior management approval,

ii. If prompted to pair with another Bluetooth device the user is to deny all requests and report such information to system administrators,

iii. The Bluetooth functionality should be turned off unless a hands-free environment is required,

iv. Data sent between paired devices must be encrypted.

15. **Desktop Redirector**: The BlackBerry Desktop Redirector may not be used.

2.9 Enterprise Data Stewardship Standard

This Standard establishes the data stewardship requirements for state agencies with the goal of protecting the confidentiality, integrity and availability of state data.

1. Data Steward(s): Each agency shall designate a data steward(s) responsible for maintaining the accuracy, privacy, and security of the data collected by the agency.

2. Necessity: Agencies shall only collect confidential customer data necessary for meeting the agency's mission and legal requirements.

3. Retention: Agencies shall only retain confidential customer data necessary for meeting the agency's mission and legal requirements.

4. Access: Agency's shall ensure that only authorized users access confidential agency information. Authorized users are those with a legitimate and necessary business need to the data.

5. Storage: Confidential data shall be securely stored. Electronic data should be stored on a centrally managed agency server if possible. Confidential data transmitted or stored outside of agency control shall adhere to the requirements of Standard 10 below.

6. Transmission: Confidential data shall be transmitted securely.

7. Training: Agency security awareness training shall include a section on protection of confidential customer information.

8. New System Development: Agencies are discouraged from using confidential data to test computer systems in development. If confidential data must be used for testing, the development system shall meet the same security standards as the production system.

9. Social Security Numbers: Collection and use of social security numbers shall be limited and based on a strong business need. Social Security numbers shall not be:

a. Used as a unique customer number.
b. Used as the primary key in databases except where required by law.
c. Displayed in full on external web-based applications beyond the initial data entry screen.

Existing systems are not subject to this requirement, however agencies are encouraged to update those systems to protect social security numbers if feasible.

10. Data Sharing: Sharing of confidential customer information outside of the agency shall be kept to a minimum. Agencies shall:

a. Have a written policy covering data sharing.
b. Require a signed, written data sharing agreement between the agency and outside entity prior to the exchange of data. The agreement shall include:

i. The data to be shared;
ii. The intended use of the data;
iii. The time period covering the exchange;

iv. The requirement that the requestor will protect the confidentiality of the data;
v. The requirement that the requestor will not re-disclose the data;
vi. The requirement that the requestor will report lost or stolen data immediately to the agency; and
vii. Provisions for final disposal of the data.

c. Maintain a record of data sharing agreements.
d. Encrypt electronic data prior to transmitting it to the sharing partner.
e. Ensure that data sharing is compliant with state and federal laws.

11. Data Publication: Agencies shall use comprehensive disclosure avoidance techniques consistent with professionally acceptable standards to de-identify confidential data before releasing it to the public.

12. Disposal: Devices and media containing confidential data shall be erased with a DoD approved method prior to disposal. Paper documents containing confidential data shall be shredded.

13. Notification: State agencies shall notify customers affected by a data breach. Notice shall be made in the most expedient time and manner possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach of security and with the legitimate needs of law enforcement.

2.10 Enterprise Information Security Compliance Standard

This standard establishes information security compliance reporting requirements for participating State of Iowa Agencies.

1. Compliance. Agencies shall comply with all State of Iowa enterprise information security standards. To comply, an agency must meet the requirement or have been granted a variance in accordance with IAC 11—25.11.

2. Reporting. Agency directors shall report annually, on a form provided by the Technology Governance Board, that they are in compliance with all State of Iowa enterprise information security standards in effect at the time of the reporting. The Agency reporting form must be completed, signed and submitted to the Technology Governance Board annually by March 15.

3. Remediation. Agencies not compliant with the enterprise information security standards shall submit a remediation plan to the Technology Governance Board annually by March 15. The remediation plan shall identify non-compliant components and a timeline for achieving compliance.

4. Verification. The DAS Information Security Office (ISO) shall conduct periodic assessments to verify that agencies are in compliance with enterprise information security standards. Assessment results will be reported to the Technology Governance Board and the ISO will recommend actions to address non-compliance.

2.11 Enterprise Web Application Security Standard

This standard provides the minimum security requirements for web applications developed, owned or managed by State agencies.

1. Social Security Numbers:

a. Social Security numbers shall not be used as a User Id or password during logon for web applications.

b. Social Security numbers shall not be displayed in full on web applications beyond the initial data entry screen

2. Development: Agencies engaged in application development must implement separate development, test, and production environments for the applications they develop. Agencies involved in application hosting must implement separate test and production environments.

a. Agencies must remove test data and accounts from production systems before these systems become live.

3. Production Data: Use of confidential data in test environments requires agency management approval.

a. Test environments using confidential data shall meet standards equivalent to the production system.

4. Coding Vulnerabilities: Agencies shall develop web applications based on secure coding guidelines and eliminate common coding vulnerabilities. At a minimum agencies must meet the current Open Web Application Security Project (OWASP) guidelines http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project to prevent:

a. Injection (SQL, LDAP, etc.)
b. Cross-Site Scripting (XSS)
c. Broken Authentication and Session Management
d. Insecure Direct Object References
e. Cross Site Request Forgery
f. Security Misconfiguration
g. Failure to Restrict URL Access
h. Unvalidated Redirects and Forwards
i. Insecure Cryptographic Storage
j. Insufficient Transport Layer Protection

5. Application Testing: Agencies shall review and test web applications for security vulnerabilities using an automated web application scanning tool. Application review shall include source code and run time analysis.

a. Web applications shall be scanned using all application roles (ex. user and admin).

b. New web applications must be scanned before going to production.

c. Existing web applications must be scanned annually and whenever significant changes are made to the application.

d. Critical/high vulnerabilities identified by the web application scans shall be remediated.

e. The web application review must be conducted by someone other than the developer.

f. The Information Security Office shall maintain a list of criteria for approved web application scanning tools.

6. Change Management: Agencies shall implement a change management procedure for deployment of agency web applications. Separation of duties shall be implemented to prevent developers from publishing their own applications to the production environment.

7. Encryption: Web applications collecting or displaying confidential data must encrypt the data in transit.

a. Data in transit shall be protected with SSL 3.1/TLS 1.0, equivalent or higher method of encryption.

8. Log-on Banner: Web applications which require a log-on shall have a log-on banner. The banner shall be approved by the agency's legal counsel and notify users that:

a. Users are entering a State of Iowa system
b. Access is limited to authorized use only
c. Users consent to monitoring

9. Access Control: User authentication is required for all web applications that collect, transmit, display or store confidential data or where the integrity of the data must be maintained. Required access controls include:

a. User ID: Each user must have a unique user ID.
b. Access Review: User group roles and rights must be reviewed at least quarterly.
c. Passwords:
  i. At least eight characters
  ii. A mixture of numbers, upper alphabetic and lower case letters
  iii. Include at least 1 special character
  iv. Changed at least every sixty days
  v. Passwords shall not be transmitted in clear text
d. Log Off: Applications shall log off users after 20 minutes of inactivity.
e. Failed Log-In:
  i. Accounts are locked after five failed login attempts within 60 minutes.
  ii. Users shall remained locked out for 24 hrs or until the account is reset by an administrator.
  iii. A message will display directing the user who to contact when this event occurs.

10. Logs: Web application logs must be collected and reviewed for security events. These logs must meet agency data retention requirements. Minimum security events to be logged include:

a. Startup and shutdown
b. Authentication
c. Authorization/permission granting
d. Process invocation
e. Unsuccessful logins
f. Unsuccessful data access attempt
g. Data deletions
h. Data transfers
i. Application configuration change

11. Application Firewall: An application firewall shall be installed in front of all external web facing applications.

12. Source Code: Access to web application source code shall be restricted to authorized employees.

13. Database: Backend databases shall not be hosted on the same physical server as web applications in production.

14. Training: Web application developers must receive technical training annually in secure coding techniques.

15. Service Providers: Agency web applications developed\hosted by an Applications Service Provider or other third party must comply with the Enterprise Web Application Security Standard http://das.ite.iowa.gov/standards/enterprise_it/index.html .

16. Inventory: Agencies must provide the Information Security Office with a list of all web applications collecting confidential information.

a. Application Name
b. URL
c. Application owner

17. Security Audits: The Information Security Office shall conduct periodic security reviews of a sample of state web applications.

CHAPTER 3 DAS OPERATING SECURITY POLICY

The DAS-ITE Operating Security Policy provides agency specific security rules which are consistent with the Enterprise Security Standards. The DAS-ITE Operating Security Policy supplements but does not replace the Enterprise Security Standards.

General Principles:

Networked computer systems are increasing in number, capability, and importance. At the same time, threats to these systems are increasing in volume and sophistication. An emphasis on information security is necessary to protect computer systems and the information they store and process. The State of Iowa is working towards providing greater access, information and services to State employees and citizens. As eGovernment increases, security becomes even more important. The Department of Administrative Services (DAS) established this operating security policy to enhance DAS security and support State information security efforts.

Compliance:

Compliance with this policy is mandatory for all DAS-ITE employees and contractors. Non-compliance may result in appropriate disciplinary actions up to and including immediate dismissal. Criminal and/or civil action against users may be appropriate where laws are violated. Where this policy differs with other established policy statements, the more current policy by date shall be enforced.

DAS-ITE management shall:

1) Provide policies, procedures, and guidelines to DAS-ITE employees.
2) Provide security training on an annual basis.
3) Provide each employee a picture identification badge.

DAS-ITE employees shall:

1) Read and follow this operating security policy.
2) Safeguard State computer resources, information, and Government buildings and property.
3) Attend security training on an annual basis.
4) Display their ID badge or a temporary badge when in DAS facilities.
5) Follow all federal and state laws that apply to computers, networks, and electronic communication.
6) Report all computer security incidents to the service desk and information security office.

Specific Policy Statements

1) Security Training

a) Security training shall be completed prior to receiving system access.

b) Employees with access to Federal Tax Information shall view the IRS training video.

c) Refresher training shall be completed annually.

d) Users who do not complete the annual security training shall have their network access revoked.

e) An acknowledgment form shall be signed by each employee and contractor attending training.

2) Physical Security

a) All doors to secure DAS-ITE areas shall be locked at all times.

b) Doors shall not be propped open unless the entryway remains controlled.

c) The vault containing warrants shall be locked at all times. Access shall be supervised by the manager, supervisor, or senior operator in charge.

d) The daily security checklist shall be completed nightly for the DAS-ITE Hoover facilities.

e) Personnel working after business hours shall not enter offices or areas not essential to duties.

f) Employees and contractors are responsible for safeguarding State computer resources, sensitive or confidential information, and Government buildings and property.

g) Cameras will monitor activity in the server room/data center.

3) Identification Badges

a) Employees – Employee and contractor access requirements shall be determined by DAS Management. The following apply to employees\contractors issued an ID access badge.

1) The badge shall be displayed with the picture visible.

2) If an employee forgets their badge they will obtain a temporary badge for that day.

3) Temporary badges shall be returned at the end of the day.

4) Personal and temporary badges shall be safeguarded by each employee.

5) Employees shall return their badges to their supervisors on their last day of employment.

6) Lost or stolen badges will be reported to supervisors within one business day.

7) Supervisors shall request an update of access rights when an employee's work schedule or job duties change.

b) Visitors - Individuals not granted badge access to a secure area shall be considered a visitor. Visitors shall be required to wear a visitor's badge while in secure DAS-ITE facilities.

1) Each visitor shall sign in and receive a visitor's badge. The visitor badge shall show the current date.

2) Visitors to areas containing Federal Tax Information (FTI) shall provide a picture ID prior to receiving a visitor badge. Vendors and contractors may not have access to areas containing FTI.

3) Each visitor shall be escorted or monitored at all times while on DAS-ITE premises by a DAS-ITE employee.

4) The visitor badge shall be displayed with the visitor indicator visible.

5) The badge issuing employee shall be responsible for instructing visitors on DAS-ITE security guidelines and how to display the badge.

6) Each visitor shall sign out and return their visitor's badge prior to departing DAS-ITE facilities.

7) The visitor log will be retained for a minimum of three months.

4) Unattended Terminals

a) Users shall lock their workstations when leaving the vicinity of their desk.

b) A password protected screensaver shall be enabled on each workstation, with the time set to no more than 15 minutes of inactivity.

c) Users shall log out of their workstations at the end of each day, unless they have a valid operational reason for leaving them logged on. If left logged on, the workstation shall be locked.

5) Consent to Monitoring

a) Use of State Government computer systems implies consent to monitoring of that usage by the Director and specific designees.

b) Computer data and information, materials and tools are to be used for work-related purposes only. Management has the right of access to employee work areas.

c) Any monitoring shall be in compliance with Iowa Code Chapter 22.

6) Use of State Computers

a) Users shall abide by the policy statements contained in the DAS Work Rules.

b) State computers shall not be used for:

1) Access to, use, or distribution of material that:

a. Is deemed obscene by a reasonable person, or

b. Would contribute to a hostile environment;

2) Seeking out unauthorized information which is private, confidential, or not open to the public;

3) Any purpose which violates US or State of Iowa law, specifically, but not limited to, Iowa Code Chapter 22;

c) Managers shall be responsible for the security and proper use of computer hardware, software, and data within their areas.

d) Managers shall be responsible for ensuring their staff has been adequately trained in basic security concepts and are aware of the policies, procedures, and guidelines concerning their use and security.

e) Computers shall not be installed, moved, removed, or connected to the network without coordinating with the DAS-ITE Service Desk.

7) Internet Use

a) Users shall abide by the policy statements contained in the DAS Internet and Email Usage, contained in the DAS Work Rules.

b) Users shall not:

1) Violate laws;

2) Interfere with network users, services, or equipment; or

3) Harass other users.

c) Personal Internet use is authorized on a limited basis as long as it does not disrupt operations, detract from work tasks, or otherwise violate DAS-ITE policy.

d) Administrator accounts shall not be used to visit the Internet except where required for system maintenance.

8) E-mail

a) Users shall abide by the policy statements contained in the DAS Internet and Email Usage Policy contained in the DAS Work Rules.

b) Confidential or sensitive information shall not be e-mailed. It is the sender's responsibility to determine the confidentiality of each e-mail sent.

c) E-mail received that is of a questionable nature, has an unusual attachment, or is not expected should not be opened. If there is any question as to the validity of an e-mail received, contact the Information Security Office.

d) Occasional e-mail of a personal nature may be sent and received as long as it does not disrupt operations, detract from work tasks, or otherwise violate DAS-ITE policy.

9) Software

a) Users shall abide by the policy statements contained in the DAS Internet and Email Usage Policy, contained in the DAS Employee Handbook.

b) Software, including shareware and freeware, from any source shall not be installed without management approval.

c) Software installation shall be coordinated with the DAS-ITE Service Desk.

d) Approved software shall be scanned for viruses prior to installation.

e) Peer-to-peer file sharing is prohibited.

f) Illegal copies of licensed software may not be installed.

10) Anti-virus Software

a) All servers, desktop and portable computers shall have current anti-virus software installed.

b) Users shall not change anti-virus software settings or otherwise interfere with the functioning of the software unless directed by a system or security administrator.

c) Users shall make every attempt to limit exposure to a virus or other malicious software.

11) User Management

a) New Users

1) Managers shall complete the New User Request Form for all new staff.

2) New users will only be granted access to systems and data needed to perform their assigned job duties.

b) Departing Users

1) Managers shall ensure that accounts are deleted when no longer necessary by completing the Departing User Request Form.

i) For the DAS-ITE LAN, accounts shall be deleted when a user terminates State employment, transfers to a different department, or no longer needs access. Accounts shall be deleted within 24 hours of departure.

ii) TSO ID: If a user transfers to a different department, terminates state employment, or no longer requires an account, their TSO ID shall be disabled and information associated with the account shall be retained. If a request has not been made within 30 days by the department to retain the ID and associated datasets, the account and associated information shall be deleted.

2) Forensic images of workstations and notebook computers will be made upon the employee's termination.

c) Changed Users

1) Managers shall complete the Changed User Request Form for all staff with a change in duties.

d) Inactive Users

1) Managers will review for inactive users at least every 90 days and remove the users where appropriate.

12) User Accounts/(IDs

a) All users shall have a unique user ID.

b) Accounts shall be locked for a period of 24 hours after 3 login failures. Authorized users may have their accounts reset by contacting the DAS-ITE Service Desk.

c) Vendor IDs - Vendor accounts should be activated only as needed.

d) Shared Accounts – The following apply to shared user accounts (such as root):

1) Accounts must be accessible only by a discrete list of users defined on the system.
2) Shared accounts will be audited by the CISO at least quarterly.
3) All users that access shared user accounts will have their access to such accounts logged.
4) Where such mechanisms are not in place, users must log their access to a shared user account by reporting access to the DAS-Information Security Office.

13) Passwords

a) Passwords for DAS-ITE computer systems and networks shall be:

1) A minimum of 8 alphanumeric characters;

2) Include at least 3 of the following.

i) Uppercase letters,

ii) Lower case letters,

iii) Special symbols, and

iv) Numbers;

3) Changed at least every 60 days with no repetitions; and

4) Protected at the highest level of information on the system.

b) Default, initial, and system passwords shall be changed immediately upon receipt.

c) Passwords for DAS-ITE computer systems and networks shall not be:

1) Written down or recorded on-line in any form;

2) Shared with anybody;

3) Words, or combinations of words, found in dictionaries, spelling lists, or other lists of words, even if combined with other alphanumeric and special characters;

4) A user ID in any form;

5) All digits or all the same letter;

6) Published examples of good passwords;

7) Information easily obtained about the user; or

8) Reused at any time.

9) Transmitted together with the User ID.

d) Certain passwords may be shared and/or written down, with management approval, in order to meet mission requirements. If a password is written down, it shall be stored and protected at a secure alternate location.

e) Non-expiring Passwords: Passwords may be set as non-expiring in certain circumstances when other security controls are put in place as compensation.

1) Approval shall be on a case by case basis by the Information Security Office and the administrator involved.

2) Other organizations affected by the decision shall be consulted and afforded the opportunity to provide input.

3) This deviation from policy shall be justified and documented.

3) Non-expiring passwords will be for newly created RACF IDs.

4) IDs with non-expiring passwords will end with a “#” (for example T123456#)

f) First-time passwords shall be set to a unique value.

14) Modems

a) Use of modems requires supervisor and CISO approval.

b) Modems on individual computers connected to analog lines shall set auto-answer to off.

c) Modems will be set to disconnect after 10 minutes of inactivity.

d) Modems will only be used in designated locations.

e) Only modems on the approved hardware list may be used.

f) An inventory of modems, their locations, and users will be maintained and audited annually by the ISO.

15) Phone/Wiring Closets

a) Phone/wiring closets shall be locked at all times.

b) Access to such closets shall be restricted to those who require it for business or maintenance purposes.

16) Hardcopy Information

a) Information in hardcopy form that is sensitive or confidential shall be stored in a secure manner when not in use.

b) Information in hardcopy form that is sensitive or confidential shall be cross-cut shredded, incinerated, or otherwise destroyed when disposed.

c) Federal Tax Information must be destroyed by burning, mulching, pulping, shredding, or disintegrating. Paper must be shredded to effect 5/16 inch wide or smaller strips; microfilm and microfiche must be shredded to effect a 1/35- inch by 3/8-inch strips.

d) It is the employee's responsibility to determine the sensitivity or confidential nature of the information before disposal. If unsure, the employee should destroy the information.

17) Mobile Devices

a) Use of personal mobile devices (BlackBerry and other PDA devices) for state business requires prior management approval. Personal devices must meet the requirements of the Enterprise Mobile Device Security Standard.

b) A list of mobile devices and users will be maintained.

c) Only mobile devices on the approved hardware list may be used.

d) Mobile devices must be password protected.

e) Personal firewalls must be installed on all mobile devices.

f) Lost mobile devices must be reported to the Information Security Office within 24

hours.

g) Mobile devices must be labeled with DAS-ITE contact information.

h) Confidential data may not be stored in mobile devices.

i) Confidential data shall not be transmitted via Short Message Service (SMS).

j) Confidential data shall not be transmitted via peer to peer messaging (PIN to PIN).

k) Employees must obtain management approval before installing third party applications on devices used to conduct state business.

l) The camera feature may not be used in areas containing confidential data.

m) The wireless functionality of devices must be disabled when in areas displaying, storing or transmitting confidential information.

n) Pairing devices requires prior management approval.

o) Data sent between paired devices must be encrypted.

18) Media and Hardware Disposal

a) All computer systems, electronic devices and electronic media must be properly cleansed of sensitive data and software before being disposed of either as surplus property or as trash.

b) Computer hard drives, including printer and copier hard drives, must be sanitized by using software that is compliant with Department of Defense standards.

c) CDs, DVDs, floppy disks, data tapes must be shredded or broken into multiple pieces.

19) Employee Screening

a) Employees and contractors must be screened by the SING system prior to receiving access to confidential data\systems or secure areas.

20) Log Review

a) Audit logs will be maintained and monitored on a daily basis for unusual or suspicious activity.

b) System managers will be responsible for reviewing the logs generated by their systems.

c) The Information Security Office will be responsible for reviewing Intrusion Detection System logs.

d) Logs will be maintained for 3 months on-line and one year offline.

e) Security camera footage will be reviewed in the event of an incident.

21) Forensics

a) A forensics investigation will be commenced within 48 hours of a compromise of a server hosting PCI data or applications.

b) Forensics investigations will be conducted for non-PCI systems at management request.

c) Forensics investigations will be conducted by Information Security Office (ISO) staff or an outside entity approved by the Information Security Office.

d) Data on DAS-ITE computers and systems may only be encrypted using ISO approved encryption software and keys.

e) Use of Disk Scrubbing Tools and File Shredding Software is prohibited except by authorized staff prior to transfer or final disposal of computer.

22) System Backup

a) Critical data stored by DAS-ITE will be backed-up daily.
1. Exchange Servers (E-mail).
2. SQL Servers (Database).

b) Mainframe data including TSO, Batch Data, and Generation Data Groups (GDG's) will be backed up monthly.

c) Other data will be backed up weekly.
1. File and Print Servers
2. Application Servers.

d) Backups will be stored off-site. A log of offsite backups shall be maintained including:
1. Date and time backup was transferred.
2. Authorization signature for the transfer.

23) Data Retention

a) This policy applies to data in electronic form including, but not limited to: electronic mail, personal calendars, instant messages, word processing and presentation documents, spreadsheets, databases, voice messages, images and photographs, videos, audio files, information on handheld devices (e.g., PDAs, Blackberry devices, and iPods), web pages, system and application logs.

b) Agency data stored on DAS-ITE systems will be subject to the respective agency's data retention policy.

c) DAS-ITE audit logs and system backups will be maintained for the following periods:

Type	**Audit Logs**	**Backups**
SQL Server (Database)	1 year	1 year
Application Server	6 months	6 months
File Server	6 months	6 months
TSO (mainframe)	6 months	6 months
Exchange (Email)	6 months	6 months
Websense	3 months	-
Intrusions Detection System	3 months	-

d). Email messages will be retained for 180 days after:
1. They are deleted.
2. A staff person leaves DAS-ITE.

e) Upon notice of pending litigation electronic information regarding the litigation will be preserved.

24) Payment Card Industry (PCI) Data Security

a) DAS-ITE follows the State of Iowa – PCI Policy Statement (see chapter 9).

b) DAS-ITE does not store or log credit cardholder information beyond the last four digits of the credit card number.

c) A list of all users with access to E-Payment system components, with the administrative privileges those users possess, will be maintained. The Access to System Components spreadsheet must be updated to show:

1. the user;
2. access granted; and
3. any administrative privileges enabled.

25) Network Connections

a) All devices connecting to the DAS-ITE network or Internet shall:

1. Change vendor supplied defaults including passwords and SNMP community strings.
2. Disable un-used ports, protocols and services.

26) Personal Data

a) User's do not have a right to privacy while using DAS-ITE computer systems.

27) Removable Storage Devices

a) Only state-owned removable storage devices may be used;
b) Removable storage devices containing confidential information must be encrypted;
c) Methods for storing/moving data on the DAS-ITE network should be used instead of storing data on removable storage devices if possible.
d) IPods and other mp3 players are prohibited from connecting to DAS-ITE computers.
e) ITE employees are responsible for the physical protection of the removable media assigned to them.
f) Removable media shall not be the primary storage device for state data. Removable media shall be backed up to agency network storage.
g) Lost removable media must be reported to the Information Security Office within 24 hours.

28) Data management
a) Data should be moved/stored using the DAS-ITE network if possible.
b) Removal of confidential or proprietary information from state computers requires:
i. A true business need;
ii. Prior management approval.
c) Production data shall not be used for application testing.
d) Confidential data shall not be emailed unless encrypted.
e) State data shall not be allowed on personally-owned devices including home computers.

29) Laptops
a) All laptops used for state business must be encrypted and meet the guidelines of the Enterprise Encryption Standard.

b) Requests for exemption from the encryption requirement may be granted by the Chief Information Security Officer.
c) Non-DAS laptops must undergo a security review before connecting to DAS-ITE computing systems.
d) ITE employees are responsible for the physical protection of the laptop assigned to them.
e) ITE laptops shall not be left unattended in an unlocked car.
f) Passwords, smart cards and tokens shall not be stored with the laptop.
g) ITE laptops shall not be the primary storage device for state data. Laptops shall be backed up to agency network storage.
h) Lost laptops must be reported to the Information Security Office within 24 hours.

30) Data Center
a) No tours will be permitted without the approval of the Data Center Manager.
b) No camera or photographic equipment will be allowed within the Data Center without the approval of the Data Center Manager.

31) Disaster Recovery/Contingency Planning
a) The agency will develop and maintain a COOP\COG plan.
b) The agency COOP\COG plan will be tested at least annually.

32) Configuration Management
a) The agency will implement a change management procedure for agency hardware and software.

32) Wireless
a) Wireless network access points connected to the ITE network must be approved by management.
b) All wireless network access points connected to agency infrastructure must be registered with the Information Security Office.
c) Access points connected to the agency network must meet the requirements of the Enterprise Wireless LAN Standard http://das.ite.iowa.gov/standards/documents/081211_wireless_LAN.pdf.
d) Access Points connected to the agency network will be scanned for vulnerabilities.
e) Client systems accessing the agency wireless must have antivirus software and up-to-date patches.
f) Public wireless shall not be used to conduct state business.

33) Data Sharing
a) Management approval is required before confidential agency data is provided to individuals outside of the agency.
b) A Data Sharing agreement must be completed for each exchange outside of the agency.
c) Confidential data shall be encrypted prior to transmission outside of the agency.

CHAPTER 4 DAS HANDBOOK AND POLICIES

DAS work rules regulate the conduct of DAS employees. Violation of the work rules provides sufficient grounds for disciplinary actions ranging from a reprimand to discharge. There are work rules specific to information security including: Computer Security; Confidentiality; Internet and Email Usage; and Visitor Security Assurance Policy.

4.1 Title: Computer Security **Work Rule Number:** 3

Staff should be aware that the computer on his or her desktop should be maintained in a secure manner. Change your password often, and do not give out your password to other workers, and do not allow anyone to use your computer with your password, unless absolutely necessary.

See your supervisor if you have any questions or concerns about the security of your computer. Remember that you have no right of privacy while using computer equipment owned by the State of Iowa.

4.2 Title: Confidentiality **Work Rule Number:** 4

Employees shall not willfully inspect (browse) confidential information and records without authorization or without a business purpose.

During your working career, you may acquire confidential information about other employees, or customers and our operations. It is vital to preserve the confidentiality of information gained by all employees. Staff members are to refrain from discussing confidential business matters outside the office, even with family members.

Additionally, some business enterprises (ITE, GSE, HRE, or SAE), will require that you sign confidentiality agreements due to the sensitive nature of information your work requires. For example, an employee’s access to taxpayer records is allowed only when information is needed to carry out their tax-administration duties. Employees are not allowed to access taxpayer records when their involvement in a tax matter could cause a possible conflict of interest, or when they have a personal relationship or an outside business relationship that could raise questions about their impartiality in handling the tax matter.

For example, employees are not authorized to initiate an access to their own records, or records of the following persons:

- Their spouse, or any ex-spouses.
- Their children.
- Their parents.
- Anyone living in the household.
- Their close relatives.
- Friends or neighbors with whom they have close relationships.
- Celebrities, when the information is not needed to carry out tax-related duties.
- An individual or organization for which they or their spouse is an officer, trustee, general partner, agent, attorney, consultant, contractor, employee or member.

- Any other individual or organization with which they may have a persona or outside business relationship that could raise questions about impartiality in handling a tax matter.

Violation of this work rule is grounds for discharge. Civil and criminal penalties may also apply.

If in doubt at any time, the employee should ask their supervisor whether an access is authorized. An employee who has had an inadvertent access occurrence needs to report the occurrence to their supervisor immediately. The supervisor will have the employee fill out an "inadvertent access" form that is signed and dated by both the employee and supervisor. Your supervisor will retain the signed form, which may be placed in your personnel file.

4.3 Title: Internet and Email Usage **Work Rule Number:** 11

Email and Internet usage are governed by these policies:

- Email at work is to be used primarily for the benefit of the Department in carrying out its mission, but a limited amount of personal email may be sent and received at work on occasion. However, personal business (for profit) and sending inappropriate materials are never forms of acceptable uses of state email.
- Supervisors may counsel and take appropriate actions with employees if, in the judgment of the supervisor, an employee is using work time and email excessively to conduct the employee's personal affairs.
- Should personal use of email by an employee result in additional costs to the State, the employee is responsible for payment of such costs.
- Internet access through the use of personal computers may be used for business, professional and education development purposes that are related to the work of the government.
- Access to the Internet and to email is a privilege and may be suspended or revoked by the employee's supervisor for violation of policy or the rules. The employee may be disciplined, up to and including discharge, for violation of the policy or the rules. Criminal and/or civil actions may be lodged against an employee who violates the policy or rules.

Employees shall use these guidelines for Internet and email use:

- Familiarize themselves with the Department's policy on Internet and email usage prior to any such use, and become familiar with and adhere to rules of etiquette and protocols in the use of the Internet and email.
- Use the State's equipment to access the Internet for government business only, not for personal business.
- Comply with applicable copyright laws, software licenses and other federal and state laws and regulations governing the use of the Internet and email.
- Shall not use the Internet or email to intentionally interfere with or disrupt other network users, network services or equipment, nor intentionally represent themselves as others.
- Shall not intentionally access, obtain, download, make use of, alter, or destroy electronic files or data that are defined as "confidential" under Iowa Code chapter 22, unless authorized to do so by the employee's supervisor.
- Shall not intentionally access, obtain, download, make use of, alter, or destroy files or data stored in the State's computer systems to which the employee has not been granted access, or intentionally alter or destroy the State's electronic files or data, unless authorized to do so in writing by the employees supervisor.

4.4 Visitor Security Assurance Policy

Visitor Security Assurance Policy – Information Technology Devices:
This policy applies to all visitors who wish to connect their information technology (IT) devices to the DAS Local Area Network (LAN). Visitors are defined as non-DAS employees, including contractors, consultants, vendor representatives and personnel from governmental entities.

DATE:
Effective Date: October 17, 2003

GOAL:
The goal of this policy is to protect the security, integrity and availability of the DAS Information Technology Enterprise (ITE) Local Area Network in those situations where IT computing devices that are not managed or controlled by DAS gain connection to the DAS LAN. This goal will be achieved by ensuring that visitor-owned IT devices meet DAS security requirements prior to connecting to the DAS network. These requirements include complying with anti-virus and security patch expectations.

In addition, when a visitor seeks to connect an IT device to the DAS LAN, a DAS employee will be required to serve as the sponsor to said request to ensure all steps are taken to meet the intent of this policy.

THREAT:
The threat of connecting non-DAS devices to the DAS LAN includes the spread of malicious software code, circumventing network protection, and increased vulnerability to system attacks.

POLICY:
This policy pertains to the connection of non-DAS managed IT devices to the DAS LAN. These IT devices include, but are not limited to, servers, laptop computers, desktop PC's, tablet PC's, and handheld computing devices. Each of these devices, its operating system and applications, are required to attain the most recent security patch level, be free of malicious software (including but not limited to virus, Trojan backdoor, spy ware), and be free from restricted applications (for example, peer-to-peer file sharing applications – see reference below). Antivirus protection must be updated on IT devices where antivirus software is available.

It is the policy of the DAS ITE Information Security Office (ISO) that, prior to being authorized to connect to the DAS LAN, all non-DAS managed computing devices will be evaluated to determine conformance with ITE security requirements.

It is presumed than any visitor (i.e. non-DAS employee) seeking to connect an IT device to the DAS LAN is conducting business on behalf of a sponsoring DAS employee. It is the responsibility of the DAS employee who is accountable for the visitor to ensure that the DAS ITE Information Security Office has been contacted prior to permitting the connection of the visitor's computing device to the DAS LAN. The accountable DAS employee will contact the DAS ITE Service Desk at (515) 281-5703 to arrange for ISO security authorization for the visitor's computing device.

COMPLIANCE:
Contact the DAS ITE Information Security Office to ensure that you are in accordance with this policy. This can be done by contacting the DAS ITE Service Desk at (515) 281- 5703 and asking for ITE Information Security Office support.

All state of Iowa employees, interns, volunteers, and contractors of participating agencies that use, develop, implement, or maintain information technology systems covered by the DAS ITE Security policy are responsible for understanding and complying with all State of Iowa enterprise information security policies, standards, processes, and procedures. This includes using, building, configuring, and maintaining systems in accordance with these policies, standards, processes, and procedures. Non-compliant situations will be brought first to the attention of the agency or the individual and efforts will be made to bring them into compliance. Depending on the severity, those who intentionally violate these policies, standards, processes, and procedures may receive disciplinary action, up to and including loss of network connectivity, immediate dismissal, and/or criminal prosecution.

All necessary expectations to this policy must be clearly documented and approved by the appropriate supervisor and the DAS ITE Information Security Office. In certain instances, agency director approval may be required.

REFERENCES:
The DAS list of restricted applications can be found here:

http://itesop.iowa.gov/desktop/Policies_and_Standards/specifically_restricted_software_list.htm

Chapter 5 State of Iowa Employee Handbook

The State of Iowa Employee Handbook (Handbook) contains work rules based on the State's collective bargaining agreements and the Iowa Department of Administrative Services – Human Resources Enterprise (DAS-HRE) rules and policies. The Handbook is applicable to all state employees including the staff of DAS-ITE.

Use of State Property

Government-owned and private property on department work sites or other state premises must be protected. Therefore, the following are prohibited: unauthorized entry to state premises; unauthorized use, abuse, misuse, or waste of property or materials; unauthorized possession or sale of items; and unlawful operation or use of state vehicles and equipment for other than state business. Some state vehicles have a GPS tracking system installed onboard. The State's long-distance service and state-owned cellular phones are to be used for official state business only. Local personal calls from state office phones must be kept to a minimum. State postage stamps and metered mail are for official business only. Employees provided access badges will not allow others to utilize the badge to permit entry to facilities, and during all work hours must prominently display the badge, not obscured by clothing or other objects, on the front upper third of the body, except when the card is being used by the employee to gain authorized electronic access to buildings, offices, facilities, or electronic communication equipment. Employees are responsible for the care and secure use of access badges provided by the employer and must, immediately upon discovery, report the loss or theft of any issued badge to management. The State's internal mail system is not to be used for the distribution or receipt of personal mail or packages. State equipment must be checked out through a management representative before removal from the premises. Equipment may not be taken off premises for employees' personal use. Personal copies made on department photocopy machines may be permitted at a charge to be set by the employing department and with the approval of the employing department.

Internet service is provided by the State of Iowa to support open communications and exchange of information, as well as to provide the opportunity for collaborative government-related work. The State of Iowa encourages the use of electronic communications by its employees. Like any resources made available to employees of the State, use of the Internet service is a revocable privilege. The use of state-provided Internet service must be for state government-related activities and not for personal business, for-profit activities, commercial advertising, entertainment, or other use that interferes with an employee's productivity or reflects poorly on state government. Individual state departments may have more specific policies in place regarding Internet usage. Misuse of the Internet, allowing others unauthorized entry to state facilities, or the unauthorized use and/or abuse of state property and equipment could be grounds for disciplinary action, up to, and including discharge. Upon termination of employment, whether voluntary or involuntary, all state equipment issued employees must be returned to the appointing authority.

CHAPTER 6 STATE LAW

Department of Administrative Services – Information Technology Enterprise staff, contractors, interns and users are also subject to state law. The following Code of Iowa sections cover the criminal and civil penalties for computer security violations.

Iowa Code §702.1A Computer Terminology.
For purposes of section 714.1, subsection 8, and section 716.6B:

1. "Computer" means an electronic device which performs logical, arithmetical, and memory functions by manipulation of electronic or magnetic impulses, and includes all input, output, processing, storage, computer software, and communication facilities which are connected or related to the computer in a computer system or computer network.

2. "Computer access" means to instruct, communicate with, store data in, or retrieve data from a computer, computer system, or computer network.

3. "Computer data" means a representation of information, knowledge, facts, concepts, or instructions that has been prepared or is being prepared in a formalized manner and has been processed, or is intended to be processed in a computer. Computer data may be in any form including, but not limited to, printouts, magnetic storage media, punched cards, and as stored in the memory of a computer.

4. "Computer network" means a set of related, remotely connected devices and communication facilities including two or more computers with capability to transmit data among them through communication facilities.

5. "Computer program" means an ordered set of instructions or statements that, when executed by a computer, causes the computer to process data.

6. "Computer services" means the use of a computer, computer system, or computer network and includes, but is not limited to, computer time, data processing, and storage functions.

7. "Computer software" means a set of computer programs, procedures, or associated documentation used in the operation of a computer.

8. "Computer system" means related, connected or unconnected, computers or peripheral equipment.

9. "Loss of property" means the greatest of the following:
    a. The retail value of the property involved.
    b. The reasonable replacement or repair cost, whichever is less.

10. "Loss of services" means the reasonable value of the damage created by the unavailability or lack of utility of the property or services involved until repair or replacement can be effected.

A person commits theft when the person:

> **Iowa Code §714.1(8).** Knowingly and without authorization accesses or causes to be accessed a computer, computer system, or computer network, or any part thereof, for the purpose of obtaining computer services, information, or property or knowingly and without authorization and with the intent to permanently deprive the owner of possession, takes, transfers, conceals, or retains possession of a computer, computer system, or computer network or any computer software or computer program, or computer data contained in a computer, computer system, or computer network.

In addition to criminal prosecution violators face civil action for unauthorized computer access.

Iowa Code §716.6B Unauthorized Computer Access -- Penalties-- Civil Cause of Action.

1. A person who knowingly and without authorization accesses a computer, computer system, or computer network commits the following:
   - a. An aggravated misdemeanor if computer data is accessed that contains a confidential record, as defined in section 22.7, operational or support data of a public utility, as defined in section 476.1, operational or support data of a rural water district incorporated pursuant to chapter 357A or 504, operational or support data of a municipal utility organized pursuant to chapter 388 or 389, operational or support data of a public airport, or a trade secret, as defined in section 550.2.
   - b. A serious misdemeanor if computer data is copied, altered, or deleted.
   - c. A simple misdemeanor for any access which is not an aggravated or serious misdemeanor.
2. The prosecuting attorney or an aggrieved person may institute civil proceedings against any person in district court seeking relief from conduct constituting a violation of this section or to prevent, restrain, or remedy such a violation.

Agencies subject to a data breach must notify individuals affected by the breach.

Iowa Code §715C.1 Definitions

As used in this chapter, unless the context otherwise requires:

1. "Breach of security" means unauthorized acquisition of personal information maintained in computerized form by a person that compromises the security, confidentiality, or integrity of the personal information. Good faith acquisition of personal information by a person or that person's employee or agent for a legitimate purpose of that person is not a breach of security, provided that the personal information is not used in violation of applicable law or in a manner that harms or poses an actual threat to the security, confidentiality, or integrity of the personal information.

2. "Consumer" means an individual who is a resident of this state.

3. "Consumer reporting agency" means the same as defined by the federal Fair Credit Reporting Act, 15 U.S.C. } 1681a.

4. "Debt" means the same as provided in section 537.7102.

5. "Encryption" means the use of an algorithmic process to transform data into a form in which the data is rendered unreadable or unusable without the use of a confidential process or key.

6. "Extension of credit" means the right to defer payment of debt or to incur debt and defer its payment offered or granted primarily for personal, family, or household purposes.

7. "Financial institution" means the same as defined in section 536C.2, subsection 6.

8. "Identity theft" means the same as provided in section 715A.8.

9. "Payment card" means the same as defined in section 715A.10, subsection 3, paragraph "b".

10. "Person" means an individual; corporation; business trust; estate; trust; partnership; limited liability company; association; joint venture; government; governmental subdivision, agency, or instrumentality; public corporation; or any other legal or commercial entity.

11. "Personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements that relate to the individual if any of the data elements are not encrypted, redacted, or otherwise altered by any method or technology in such a manner that the name or data elements are unreadable:

a. Social security number.

b. Driver's license number or other unique identification number created or collected by a government body.

c. Financial account number, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account.

d. Unique electronic identifier or routing code, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

e. Unique biometric data, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data.

"Personal information" does not include information that is lawfully obtained from publicly available sources, or from federal, state, or local government records lawfully made available to the general public.

12. "Redacted" means altered or truncated so that no more than five digits of a social security number or the last four digits of other numbers designated in section 715A.8, subsection 1, paragraph "a", is accessible as part of the data.

Iowa Code §715C.2 SECURITY BREACH == CONSUMER NOTIFICATION == REMEDIES.

1. Any person who owns or licenses computerized data that includes a consumer's personal information that is used in the course of the person's business, vocation, occupation, or volunteer activities and that was subject to a breach of security shall give notice of the breach of security following discovery of such breach of security, or receipt of notification under subsection 2, to any consumer whose personal information was included in the information that was breached. The consumer notification shall be made in the most expeditious manner possible and without unreasonable delay, consistent with the legitimate needs of law enforcement as provided in subsection 3, and consistent with any measures necessary to sufficiently determine contact information for the affected consumers, determine the scope of the breach, and restore the reasonable integrity, security, and confidentiality of the data.

2. Any person who maintains or otherwise possesses personal information on behalf of another person shall notify the owner or licensor of the information of any breach of security immediately following discovery of such breach of security if a consumer's personal information was included in the information that was breached.

3. The consumer notification requirements of this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation and the agency has made a written request that the notification be delayed. The notification required by this section shall be made after the law enforcement agency determines that the notification will not compromise the investigation and notifies the person required to give notice in writing.

4. For purposes of this section, notification to the consumer may be provided by one of the following methods:

a. Written notice to the last available address the person has in the person's records.

b. Electronic notice if the person's customary method of communication with the consumer is by electronic means or is consistent with the provisions regarding electronic records and signatures set forth in chapter 554D and the federal Electronic Signatures in Global and National Commerce Act, 15 U.S.C. } 7001.

c. Substitute notice, if the person demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars, that the affected class of consumers to be notified exceeds three hundred fifty thousand persons, or if the person does not have sufficient contact information to provide notice. Substitute notice shall consist of the following:

(1) Electronic mail notice when the person has an electronic mail address for the affected consumers.

(2) Conspicuous posting of the notice or a link to the notice on the internet web site of the person if the person maintains an internet web site.

(3) Notification to major statewide media.

5. Notice pursuant to this section shall include, at a minimum, all of the following:

a. A description of the breach of security.

b. The approximate date of the breach of security.

c. The type of personal information obtained as a result of the breach of security.

d. Contact information for consumer reporting agencies.

e. Advice to the consumer to report suspected incidents of identity theft to local law enforcement or the attorney general.

6. Notwithstanding subsection 1, notification is not required if, after an appropriate investigation or after consultation with the relevant federal, state, or local agencies responsible for law enforcement, the person determined that no reasonable likelihood of financial harm to the consumers whose personal information has been acquired has resulted or will result from the breach. Such a determination must be documented in writing and the documentation must be maintained for five years.

7. This section does not apply to any of the following:

a. A person who complies with notification requirements or breach of security procedures that provide greater protection to personal information and at least as thorough disclosure requirements than that provided by this section pursuant to the rules, regulations, procedures, guidance, or guidelines established by the person's primary or functional federal regulator.

b. A person who complies with a state or federal law that provides greater protection to personal information and at least as thorough disclosure requirements for breach of security or personal information than that provided by this section.

c. A person who is subject to and complies with regulations promulgated pursuant to Title V of the Gramm=Leach=Bliley Act of 1999, 15 U.S.C. } 6801=6809.

8. a. A violation of this chapter is an unlawful practice pursuant to section 714.16 and, in addition to the remedies provided to the attorney general pursuant to section 714.16, subsection 7, the attorney general may seek and obtain an order that a party held to violate this section pay damages to the attorney general on behalf of a person injured by the violation.

b. The rights and remedies available under this section are cumulative to each other and to any other rights and remedies available under the law.

Iowa Code §715C.3. DISCLOSURE OF PERSONAL INFORMATION BY PUBLIC OFFICIALS, ENTITIES, OR AFFILIATED ORGANIZATIONS == INTERIM STUDY COMMITTEE REQUESTED. The legislative council is requested to establish an interim study committee to assess and review the extent to which public officials, entities, and affiliated organizations in possession of or with access to personal identifying information of a resident of this state which could, if disclosed, render the resident vulnerable to identity theft, are disclosing or selling such information for compensation. Based upon this assessment and review, the committee shall develop recommendations relating to these practices. The committee shall be composed of ten members representing both political parties and both houses of the general assembly. Five members shall be members of the senate, three of whom shall be appointed by the majority leader of the senate and two of whom shall be appointed by the minority leader of the senate. The other five members shall be members of the house of representatives, three of whom shall be appointed by the speaker of the house of representatives and two of whom shall be appointed by the minority leader of the house of representatives. The committee shall issue a report of its recommendations to the general assembly by January 15, 2009.

CHAPTER 7 PHYSICAL SECURITY

The Department of Administrative Services – Information Technology Enterprise (DAS-ITE) is located in B level of the Hoover State Office Building with a redundant backup site at the Joint Forces Headquarters (JFHQ). Additional ITE equipment is located at the Lucas State Office Building.

7.1 Building Descriptions

Hoover Building

The Hoover Building is open to the public Monday through Friday from 7:00 a.m. through 5:00 p.m. State Patrol Post 16 (Capitol Police) patrols the building at night.

Remote controlled cameras are located inside and outside the building entrances. All cameras can be viewed by State Patrol Post 16. The cameras record 24 hours a day, seven days a week. Additional cameras are located throughout the DAS-ITE server room /data center. Additional cameras may be installed as authorized by management.

The Hoover Data Center monitors temperature, humidity and power. Alerts are sent to designated staff if problems are detected. A FM200 fire suppression system protects the data center.

During 2nd shift, the entire DAS-ITE area on B level is reviewed by a computer room employee using a physical security checklist. Most of the items on the checklist relate to doors being properly closed and locked. Coffee pots or fans left on at the end of the day are turned off as well as any PC monitors. The unusual conditions of this daily security walk-through are e-mailed to the data center manager.

Joint Forces Headquarters (JFHQ)

The Joint Forces Headquarters Building provides a data center for state agencies. Access to JFHQ is monitored by armed security guards. The guards monitor video cameras located throughout the building and process visitors to the building.

Two server rooms are available to state government. All server cabinets are locked within the data center.

The Camp Dodge facilities manager monitors temperature, humidity and power for the JFHQ building. A FM200 fire suppression system is used in the data center.

Lucas Building

Additional ITE equipment is housed in the ICN data center at the Lucas State Office Building. Access to the ICN data center is managed by the ICN Service Desk.

7.2 Access Control System

Access to state capitol complex buildings is by access card\ID badge. Agencies assign access cards to permanent and contract employees based on the agency’s security policy. Cards are programmed to open specific building/office doors and parking lot gates.

Supervisors initiate the request for an access card. The written request is completed and signed by the authorized individuals in the agency. The request is then sent to Public Safety for processing.

Access cards may be updated at the request of a supervisor without the card being physically present. When an access card is used to open a door the event is logged. Reports may be obtained from Public Safety on all agency access cards.

DAS-ITE access cards are used by employees to access secure areas (offices and data center) on Hoover B and A level.

JFHQ has a separate access badge system. Requests for access to JFHQ are initiated by the employee’s supervisor and processed by JFHQ staff.

7.3 Visitor Access

Visitors are required to sign in and are given a visitor badge to be worn at all times while in the DAS-ITE data center. Visitors must be escorted or monitored while in the data center.

Visitors to JFHQ sign in at the reception desk. Visitors must provide ID before being escorted in the data center.

ITE employees must submit a service desk ticket to the ICN before gaining access to the Lucas Data Center. Visitors must phone the ICN service desk upon entering and exiting the data center.

7.4 Safe

A fireproof safe is used at the Hoover data center for secure storage of keys, documents, and backups. Staff members with knowledge of the safe combination are: the data center manager, the three shift managers, and the three shift lead workers.

CHAPTER 8 Computer Security Incident Response

8.1 Purpose

A timely coordinated response to information security incidents can limit the duration and severity of the incident. The incident response procedure establishes a uniform process for reporting and responding to computer security incidents.

8.2 Scope

This guide is applicable to incidents investigated by the Information Security Office.

8.3 Incident Reporting

Information security incidents should be reported to the employee's supervisor and Service Desk which will forward them on to Information Security Office staff. Incidents may also be identified using the ISO's resources such as the Intrusion Detection System (IDS) and Security Event & Information Management System (SEIM).

Information Security Office staff will complete an Incident Report located in N:\Information Technology\Information Security\Incidents. The incident should also be added to the incidents.xls spreadsheet.

8.4 Information Gathering

Information Security Office staff will form an incident response team to gather information regarding the incident. ISO will maintain a neutral posture during the investigation and not assign blame for the incident. Efforts should be made to avoid creating a false sense of urgency during the investigation.

If additional information is needed regarding potential staff misuse of systems/data ISO staff will work with the employee's supervisor to gather the information.

Additional information may be requested to assist with the analysis. Additional information may include:

- Application or network logs.
- The computer or device targeted by the incident.

If computer equipment is collected during the investigation a chain of custody form shall be completed. The form is located at N:\Information Technology\Information Security\Incidents\Computer Receipt.doc.

8.5 Containment

If the security incident appears to be on-going efforts will be made to contain the incident. Depending on the nature of the incident ITE email and networking staff may be asked to contain the spread of the computer security incident. Containment efforts may include, but is not limited to:

- Blocking traffic to affected ports.
- Blocking traffic from specified IP addresses.
- Blocking email attachments with specified file extensions.
- Blocking messages with specified subject lines.
- Disconnecting devices from the shared IT infrastructure.

8.6 Summary

An incident summary will be prepared. If the incident may involve employee misuse of systems or data then the summary will be shared with the employee’s supervisor. The summary shall include a description of the incident, methods of investigation, general conclusions and recommendation.

A detailed report including a full description of the incident and activities engaged to minimize the impact of the incident will also be written. This report will include the initial notification; verification of the incident; communication among agencies; steps taken to minimize the incident; and recommendations for prevention of future incidents.

The incident shall be classified by its extent. The two categories are:

Local: Incidents localized to a single agency. Patterns of these incidents may be indicators of future activity. Examples include:

- Localized malicious code.
- Minor attempts at intrusion and reconnaissance.
- Theft of IT devices.
- Denial of Service (single agency).
- Financial fraud involving computers.
- Unauthorized activity involving a file server or host.
- Unauthorized access to personally identifiable information.
- Internet abuses which violate either Federal or State law.
- Web Defacement.

Enterprise: Incidents state-wide. These incidents involve multiple agencies. Examples include:

- Worm outbreak.
- Denial of Service (multiples agencies).

8.7 NOTIFICATION

Law enforcement
Law enforcement will be contacted if an incident appears to involve criminal activity.

- If the incident is on the capitol complex, the Iowa State Patrol Post 16 (515-281-5608) will be contacted.

- If the incident is off the Capitol Complex, the Iowa Division of Criminal Investigation (515-281-5138) will be contacted.

- If the incident involves child pornography the Iowa Division of Criminal Investigation will be contacted. Gerard Meyers 515-965-7402 or Nate Teigland 712-328-4870.

- The Federal Bureau of Investigation (FBI) should be contacted if:
    - Unauthorized entry occurred and damages equal or exceed $5,000.
    - The security incident appears to have foreign government sponsorship.
    - The security incident appears to have a terrorist connection.

  Des Moines RA @ 515 223 4278 or Brian Endrizal endrizal@dps.state.ia.us

PCI
The State Treasurer's Office must be notified if the incident involves credit card holder information. Randi McLaughlin-Tank at 515-281-6093.

Social Security Administration
The Social Security Administration (SSA) must be notified if the incident involved social security data.

Leah Ann McCormick
Program Specialist, Center for Programs Support
601 E. 12th Street, Room 460
Kansas City, MO, 64106

Phone Number: 816-936-5655
Fax Number: 816-936-5951
Email Address: leah.ann.mccormick@ssa.gov

If the SSA Regional Office cannot be reached the SSA's Network Customer Service Center (NCSC) will be contacted: 410-965-7777 or 1-888-772-6111.

Internal Revenue Service
The Internal Revenue Service (IRS) must be notified if the incident involved tax payer information. Contact the Agent-in-Charge, Treasury Inspector General for Tax Administration (TIGTA).

Treasury Inspector General for Tax
Administration
Ben Franklin Station
P.O. Box 589
Washington, DC 20044-0589

1-800-366-4484

Individuals

Iowa Code Chapter 715C requires that individuals be notified if their personal information has been disclosed. See sample breach notification. The breach notification letter and press release shall also be posted to the DAS website.

Internet Service Providers

Internet service providers should be contacted for incidents such as distributed denial of service attacks (DDoS).

- ATT

- Iowa Communications Network (ICN)
  ICNServiceDesk@iowa.gov
  1-877-426-4692
  (515) 323-4400

Internet Search Engines

Internet search engines such as Google should be contacted if confidential information has been posted to the Internet. The search engines should be asked to remove the confidential information from their index/cache.

Google https://www.google.com/webmasters/tools/removals?pli=1

Agencies

ITE and agency work teams affected by the incident shall be contacted. Initial agency notifications shall go to the Information Security Officer.

Chapter 9 DAS-ITE – PCI Policy

Introduction

The State of Iowa provides goods and services to its customers and accepts credit cards as one form of payment. The State Treasurer of Iowa contracts with a merchant service provider (currently US Bank/Elavon) to serve as the acquiring bank for the State of Iowa. State agencies act as merchants under the Treasurer of State's agreement with the merchant service provider.

The Department of Administrative Services - Information Technology Enterprise (DAS-ITE) supports the Epayment Engine which was established to promote web-based financial transactions for the State. The Epayment Engine facilitates on-line credit card transactions.

The purpose of this PCI policy statement is to establish requirements:

- Promoting security in the collection, maintenance, and transfer of credit card data;
- Ensuring compliance with the Payment Card Industry (PCI) Data Security Standards.

The primary focus of the PCI Data Security Standards is helping merchants (such as state agencies) improve the security of cardholder information by improving their overall security. Improvement in overall security will reduce the chances of security breaches and unintended disclosure of cardholder information. Compliance with the PCI Data Security Standards is necessary to improve the integrity and security of the credit card payment system. Compliance with the PCI Data Security Standards is also a requirement under the Treasurer of State's contract with the merchant service provider.

Approval

Agencies that want to accept credit cards should contact the Treasurer's Office. The Treasurer's Office obtains a merchant ID number for the agency from US Bank/Elavon and if the agency plans to accept in-person, mail or phone orders, the Treasurer's Office orders the proper equipment.

Agencies wanting to accept credit card payments online also complete ITE's customers Intake Form to begin the process to accept credit card payments via the agency's website.

Standards

DAS-ITE shall adhere to PCI Data Security Standards for credit card services including:

1. Training: DAS-ITE shall ensure that all employees responsible for systems, processes or procedures related to credit card transactions or data have completed training in the PCI-DSS requirements. DAS-ITE shall also provide security training to all employees to ensure adherence to PCI Standards and their agency's security policies.

2. Outsourcing Agreements with Third-Party Providers

Agencies contracting with third party providers for part of their credit card processing must ensure that those providers are compliant with the PCI Standards. Agencies are responsible for breaches resulting from non-compliant third party providers.

a. Payment Processing Service: The State of Iowa has a Master Services Agreement (MSA) with the merchant services provider (currently US Bank/Elavon). The merchant services provider offers merchant card payment processing services for agencies accepting credit card payments.

b. Epayment Engine: ITE's Epayment Engine provides services to transmit credit card information from agency websites to the payment gateway.

DAS-ITE does not contract with third party providers for credit card processing.

3. Data and System Security: DAS-ITE does not store or log credit cardholder information beyond the last four digits of the credit card number. DAS-ITE adheres to the following PCI-DSS data and system security requirements for credit card merchant services:

Firewalls

- Maintain firewalls between systems processing or storing credit card information and all other systems and external connections.
- Configure firewalls to deny all traffic not specifically allowed.
- Implement dynamic packet filtering.

System Settings

- Change or disable vendor default security settings (ex. default accounts and passwords) prior to installing systems on the network.
- Harden production systems by removing all unnecessary functionality, services and protocols.
- Use secure, encrypted communications for remote administrative access.

Stored Data Protection

- Dispose of sensitive cardholder data when it is no longer needed.
- Do not store the full contents of any track from the magnetic stripe in any manner.
- Do not store the card-validation code in any manner.
- Mask all but the last four digits of the account number when displaying cardholder data.
- Account numbers must be securely stored by means of encryption or truncation.
- Account numbers must be truncated to the last four digits before being logged in the audit trail.
- Access to card account numbers must be restricted to users on a need-to-know basis.
- Cardholder data may not be copied to local hard drives, removable media or mobile devices.

Transmitted Data Protection

- Transmissions of sensitive cardholder data must be encrypted through the use of SSL.
- Unencrypted credit card numbers may not be transmitted via email or FTP.

Anti-Virus Protection

- All servers and workstations must have antivirus software installed and running.
- Anti-virus software must automatically check for updates at least daily.
- Generate and monitor anti-virus audit logs.

Applications and Systems Security

- All systems must be updated with the latest security patches.
- Critical patches, as identified by the Information Security Office, must be applied within 5 business days of their release. Non-critical security patches must be applied within one month of release.
- The software development process must be based on industry best practice and information security must be included throughout the software development lifecycle.
- Sensitive cardholder data must be sanitized before it is used for testing and development.
- All changes must be formally tested, authorized, planned and logged.
- Sensitive cardholder data stored in cookies must be secured or encrypted.
- Web applications accepting cardholder data must be scanned for vulnerabilities by the security team prior to release to production.

Account Security

- System administrator will limit staff access to cardholder information.
- All users must authenticate using a unique user ID and password.
- Remote access must be via a secure connection, for example the VPN.
- All passwords must be encrypted.
- All user accounts must be revoked immediately upon termination.
- All user accounts must be regularly reviewed to ensure that malicious, out-of-date and unknown accounts do not exist.
- All inactive accounts must be automatically disabled after 60 days.
- Vendor accounts used for remote maintenance must be disabled when not needed.
- Group, shared or generic accounts are prohibited.
- Passwords must be changed on a regular interval, every 60 days or less.
- Passwords must follow strong password conventions and must not be allowed to be reused for at least a year.
- Multiple password attempts or brute force attacks must result in an account lockout.

Physical Access

- Multiple physical security controls must be implemented to prevent unauthorized access.
- Equipment and media containing cardholder data must be physically protected against unauthorized access.
- Cardholder data printed on paper or received by fax must be protected against unauthorized access.
- Secure procedures for the distribution and disposal of any media containing cardholder data must be followed.
- All media devices that store cardholder data must be inventoried and properly secured.

- Cardholder data must be deleted or destroyed before it is physically disposed (e.g. by shredding paper and degaussing media).

Access Tracking

- All access to cardholder data must be logged.
- Logs must contain successful and unsuccessful login attempts and all access to the audit logs.
- Critical system clocks must be synchronized and logs must include date and time stamps.
- Logs must be secured, regularly backed up and retained for three months online and one year offline.

Employee Screening

- Employee information will be entered in the SING background check system for screening prior to receiving access to systems containing cardholder data.

System Security Testing

- Conduct penetration tests annually.
- Deploy intrusion detection system(s).
- Deploy integrity monitoring software.

4. PCI Compliance: DAS-ITE shall be in compliance with the Payment Card Industry (PCI) Data Security Standards. If DAS-ITE becomes non-compliant with the PCI Data Security Standard, the ability to accept payments by credit card will be revoked by the State Treasurer until a compliant status is attained.

5. Risk & Vulnerability Assessment: DAS-ITE is required to complete the PCI self-assessment questionnaire annually and perform quarterly PCI Security Scans for all externally-facing IP addresses. Scans shall also be performed after significant changes to the environment. DAS-ITE will address any issues identified in the questionnaire and scans.

6. Fines and Penalties: State agencies have final responsibility for being in compliance with the Payment Card Industry (PCI) Data Security Standards. If the agency does not comply with the security requirements or fails to rectify a security issue, the payment card industry may:

- Fine the responsible merchant.
- Impose restrictions on the merchant.

7. Loss or Theft of Account Information: DAS-ITE must immediately report suspected or confirmed loss or theft of any material or records that contain cardholder data to the Information Security Office and Treasurer of State's Office. Failure to immediately notify the proper authorities will put the agency at risk of a penalty of $100,000 per incident. If found non-compliant at the time of a breach agencies are subject to fines by the payment card industry, of up to $500,000 per incident. In addition, agencies shall pay the costs associated with any investigation, data loss, chargeback fees, compliance audits, in addition to any remediation costs.

The Treasurer of State's Office will notify the merchant service provider of the loss or theft of credit card data. The offending agency will notify individuals whose credit card information was compromised.

Review

The DAS-ITE PCI Security Policy and enterprise security policies will be reviewed annually by the Information Security Office and updated as appropriate.

State of Iowa Security Policies

DAS-ITE shall adhere to the State of Iowa Enterprise security policies and develop its own internal security policies. The Enterprise Security policies are located at: http://das.ite.iowa.gov/standards/enterprise_it/index.html

Exclusions

There are no exclusions or exceptions to this policy. Staff, contractors and other personnel; or others that use systems or networks supported by DAS-ITE shall abide by these policies. These policies pertain to credit card payments processed by the DAS-ITE. All servers or databases housed at DAS-ITE that receive, store, or transmit credit card numbers are subject to these policies.

Effective Date

This policy shall be effective October 1, 2007.

Glossary

Acquirer (Acquiring Bank) – Bankcard association member that initiates and maintains relationships with merchants that accept payment cards

Cardholder – An individual who appropriately uses a payment card for purchases.

Credit Card Number – A unique number used in a financial transaction that identifies a particular credit card account.

Encryption – The process of securing electronic data transmission through the encoding of transaction information.

Merchant – An agency or unit that is authorized to accept credit card payments for goods or services provided to customers.

Merchant Number – A unique number that identifies an agency department or unit that is an approved merchant.

Payment Card Industry Data Security Standards (PCI-DDS) – The compliance requirements that have been established by the leading card associations with the objective of improving the safekeeping of cardholder information and the prevention of system breaches.

Point of Sale (POS) Terminal – A computer terminal functioning as a standalone system or connecting to a server and that is used for authorizing and processing sales transactions.

Service Provider - Business entity that is not a payment card brand member or a merchant directly involved in the processing, storage, transmission, and switching or transaction data and cardholder information or both. This also includes companies that provide services to merchants, services providers or members that control or could impact the security of cardholder data. Examples include managed service providers that provide managed firewalls, IDS and other services as well as hosting providers and other entities. Entities such as telecommunications companies that only provide communication links without access to the application layer of the communication link are excluded.

Chapter 10 DAS-ITE – Mainframe Security Policy

Introduction

The State of Iowa provides goods and services to its customers for Mainframe IBM Z/OS processing. This includes hardware and third party software. The security software package that is used is IBM's Security Server Resource Access Control Facility (RACF).

The purpose of this policy statement is to establish requirements:

- Promoting security for data;
- Ensuring compliance with Audit Standards.

Security Server RACF

IBM's Security Server Resource Access Control Facility (RACF) protects mainframe resources by granting access only to authorized users. RACF retains information about users, resources, and access authorities in special structures called profiles. RACF provides the ability to:

- Identify and authenticate users,
- Authorize users to access protected resources,
- Log and report various attempts of unauthorized access to protected resources,
- Control the means of access to resources, and
- Allow applications to use the RACF macros.

It's the responsibility of the agency to request protection of their resources.

User Access

User access is reviewed. Security ID's are deleted if:

- The State Employee is not on the State Payroll, or
- The ID has been inactive for 18 months.

If it is a Department of Human Service's (DHS) ID, the information is reported to DHS and no action is taken until DHS requests it.

System Review

The RACF exception reports are reviewed daily and exceptions are reported to the proper personnel for appropriate action.

GLOSSARY

Access

Ability to make use of any information system (IS) resource.

Authenticate/Authentication

1) The process to verify the identity of a user, device, or other entity in a computer system, often as a prerequisite to allowing access to resources in a system.

2) A process used to verify that the origin of transmitted data is correctly identified, with assurance that the identity is not false. To establish the validity of a claimed identity.

Authorization

The privileges and permissions granted to an individual by a designated official to access or use a program, process, information, or system. These privileges are based on the individual's approval and need-to-know.

Availability

Ensuring timely and reliable access to and use of information.

Compromise

The disclosure of sensitive information to persons not authorized access or having a need-to-know.

Confidentiality

The property that sensitive information is not disclosed to unauthorized individuals, entities or processes.

Critical Assets

Those assets which provide direct support to the organization's ability to sustain its mission. Assets are critical if their absence or unavailability would significantly degrade the ability of the organization to carry out its mission, and when the time that the organization can function without the asset is less than the time needed to replace the asset.

Encryption

The conversion of plaintext or data into unintelligible form by mean of a reversible translation that is based on a translation table or algorithm.

Firewall

A gateway that limits access between networks in accordance with local security policy.

Information Security

The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

Integrity

The property that sensitive data has not been modified or deleted in an unauthorized and undetected manner.

Label

The marking of an item of information that reflects its information security classification.

Least Privilege

The principle that requires each subject be granted the most restrictive set of privileges needed for the performance of authorized tasks. The application of this principle limits the damage that can result from accident, error, or unauthorized use.

Malicious Code

Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host.

Network Security

Protection of networks and their services from unauthorized modification, destruction, or disclosure, and the provision of assurance that the network performs its critical functions correctly and there are no harmful side-effects.

Security Incident

A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. Security Incidents pose a threat to the shared State IT infrastructure with respect to confidentiality, integrity, or availability.

Threat

Any circumstance or event with the potential to adversely impact agency operations (including mission, functions, image, or reputation), agency assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service

Vulnerability

A weakness, or finding that is non-compliant, non-adherence to a requirement, a specification or a standard, or unprotected area of an otherwise secure system, which leaves the system open to potential attack or other problem.

Appendix A

ROLES AND RESPONSIBILITIES

Enterprise Information Security Office

Under the auspices of the Department of Administrative Services and under the leadership of the Chief Information Security Officer, the Information Security Office develops and implements an enterprise risk management program, publishes enterprise level security policies, standards, processes, and procedures, and provides programs and processes to facilitate the implementation of this policy. The Information Security Office will serve as a central coordinating group to establish cyber security response procedures, ensure that best practices are shared, coordinate training and act as a catalyst to improve overall cyber security across state government.

It also coordinates the development of security service offerings and functions to ensure needed security services are available to Iowa government-related entities. The Chief Information Security Officer is responsible for maintaining a relationship with agencies, coordinating relevant information flow between the agency and the Information Security Office, and disseminating appropriate information throughout the Enterprise.

Agency Director

Agency directors (or equivalent), in coordination with their Chief Information Officer and Division Administrators, are ultimately responsible for the implementation of the enterprise information security policy in their agency and the development and implementation of agency security policies, standards, processes, and procedures. Agency directors also formally appoint primary and alternate agency security officers to function as liaisons to the Information Security Office.

Agency CIO

Each agency Chief Information Officer coordinates with their director, security officer, and other management personnel to ensure the implementation of the enterprise information security policy. They also develop and implement agency security policies, standards, processes, and procedures. Each Chief Information Officer is responsible for implementing an information technology program that includes security measures meeting or exceeding enterprise security policies, standards, processes, and procedures.

Agency Security Officer

Each agency's security officer coordinates with the agency Chief Information Officer and other management personnel to ensure the implementation of the enterprise information security policy in their agency, including the development and implementation of agency security policies, standards, processes, and procedures. The security officer is responsible for maintaining a relationship with the Information Security Office, coordinating relevant information flow between the agency and the Information Security Office, and disseminating appropriate information throughout the agency. The security officer is the Information Security Office's main point of contact within each agency.

Agency Managers/Supervisor

Managers and supervisors are responsible for ensuring their staff members know and understand appropriate security policies, standards, processes, and procedures.

User

Each user shall, within their capabilities, protect information and system/network resources against occurrences of sabotage, tampering, denial of service, fraud, misuse, or release of information to unauthorized persons. This includes protecting passwords and other account information; following appropriate policies, standards, processes, and procedures; and notifying appropriate authorities when incidents occur.

Data Owner

Data owners (as defined by agency management) are responsible for authorizing access to data. Data owners approve all accesses to resources under their responsibility, judge the asset's value and label the data as such, and ensure compliance with applicable controls through regular review of data classification and authorized access. Data owners also assist in assessing the risks to the confidentiality, integrity, and availability of applicable information and information resources.

System Administrator

The term "system administrator" is used here in the general sense, and includes system, network, firewall, and other technology administrators that provide technical support to specific systems or networks. System administrators monitor performance, provide problem determination and production support, and perform system back-ups. Security-related responsibilities include, but are not limited to, ensuring that:

- applicable patches, service packs, and updates are installed;
- only authorized software is installed via authorized means;
- systems are developed and implemented in a secure manner, following established enterprise security policies, standards, processes, and procedures;
- approved security procedures are followed and established where necessary;
- systems are recovered in a secure manner;
- ad hoc system reviews are performed to identify unusual activity;
- security administrators are notified of changes to software that might impact system security features before installation of those changes; and,
- procedures for software license validation and virus testing have been followed.

Security Administrator

Security administrators provide security-related administration tasks for critical systems. Where practical, separate system and security administration functions should exist, but in every case, both system and security administrative functions must be performed. When the system and security administration functions are performed by the same individual, care should be taken to ensure a secure approach is utilized. Security administration responsibilities include, but are not limited to:

- development and implementation of system-specific security policies, standards, processes, and procedures;
- authentication (add, change, delete) services;
- authorization (add, change, delete) services to provide access to applications;
- generation and distribution of reports for monitoring access and potential security breaches; and,
- developing incident handling procedures.

Database Administrator

Database administrators ensure the confidentiality, integrity, and availability of databases under their control. Security responsibilities include, but are not limited to:

- designing, developing, organizing, managing, and controlling databases in accordance with applicable security policies; and,
- recovering databases in a secure manner when damaged or compromised.

Application Developer

Application developers develop secure applications consistent with established policies, standards, processes, and procedures. Applications shall protect individual privacy, the confidentiality of electronic commerce information, and the integrity of both the information it processes and the application itself. Applications must log significant security events, protect the log files appropriately, and prevent co-mingling of data within the application.

Appendix B

Sample Breach Notification

Date

Name
Address
City, State Zip

Dear [Name];

I am writing to provide you notice of a recent data breach at the [agency name] affecting your personal information.

[Insert a description of the data breach. Include the:

- Date of the breach;
- Brief overview of the breach;
- Information released by the breach (i.e. name, social security number, date of birth etc.); and
- Remediation efforts on the part of the agency.]

The [agency name] is unaware of any incident of identity theft related to this breach however you may place a 90 day fraud victim alert on your credit report by contacting the following credit reporting companies.

Equifax	Experian	TransUnion
P.O. Box 740241	P.O. Box 9532	P.O. Box 6790
Atlanta, GA 30374-0241	Allen, TX 75013	Fullerton, CA 92834-6790
800-525-6285	888-397-3742	800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

You should remain vigilant about possible identity theft or fraud in the future. To obtain a free annual copy of your credit report, go to www.annualcreditreport.com, or call toll-free to 1-877-322-8228.

For more information about protecting yourself from identity theft please visit http://www.ftc.gov/bcp/edu/microsites/idtheft/.

We regret that this incident has occurred.

Sincerely,

Appendix C

Acknowledgment of Receipt for the ITE Security Policy Manual

I acknowledge receipt of the Department of Administrative Services – Information Technology Enterprise Security Policy Manual. I am aware that I am expected to read and be familiar with the information contained in this handbook. Further, I understand that I am subject to and shall comply with each and every security policy including:

- Enterprise Security Standards
- DAS Operating Security Policy
- DAS Work Rules
- DAS Operating Procedures

Employee/Contractor/Intern Signature	Supervisor Signature
Employee/Contractor/Intern Name (Printed)	Supervisor Name (Printed)
Date	Date